WOODBRIDGE SCHOOL

Online Safety (E-Safety) Portfolio Policy – Whole School

Version Number:	V 2.0
Applies to:	Whole School (including EYFS)
Author (s):	Deputy Head (Pastoral), Head of Online Safety
Review Frequency:	Annual
Policy category (1, 2, 3, 4):	2
Last reviewed:	Trinity Term 2021 (small updates Lent Term 2022)
Next review due by:	Trinity Term 2022
Approved on (date):	Michaelmas term 2020 (by School Committee) and then updated Trinity Term 2021
Committee (s) Responsible:	Education
References (including legal and others eg ISBA).	DfE Preventing and Tackling Bullying: DfE: Supporting children and young people who are bullied: Advice for Schools; DfE Keeping Children Safe in Education; DfE Searching, Screening and Confiscation
ISI Reg:	7h
Other related policies and documents:	Behaviour Management; Data Protection Policy; Acceptable Use Policy; EYFS Policy; Safeguarding & Child Protection Policy; Bullying Policy; Complaints Policy; Social Media Policy; CCTV Policy; BYOD Policy; Staff Behaviour Policy; health and Safety Policy; PSCHEE

Please note: All *amendments to policies within this portfolio approved by School Committee on 5 May 2020 to reflect changes required for COVID-19.*

Contents

This policy portfolio covers the whole of the School organisation, including Woodbridge School, Woodbridge School Prep and Early Years Foundation Stage. It has been drawn up on the advice of professionals in the areas, external agencies and in liaison with pupils.

1. Introduction

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

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

- ☐ Websites;
- ☐ Email and instant messaging;
- ☐ Blogs;
- ☐ Social networking sites;
- ☐ Chat rooms;
- ☐ Music / video downloads;
- ☐ Gaming sites;
- ☐ Text messaging and picture messaging;
- ☐ Video calls;
- ☐ Podcasting;
- ☐ Online communities via games consoles; and
- ☐ Mobile internet devices such as smart phones and tablets.

This policy, supported by the Acceptable Use policy (for all staff, visitors and pupils), is implemented to protect the interests and safety of the whole School community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following School policies:

- ☐ Safeguarding;
- ☐ Staff Behaviour;
- ☐ Health and Safety;
- ☐ Behaviour Management;
- ☐ Anti-Bullying;
- ☐ Acceptable Use Policy;
- ☐ Social Media;

- ☐ Data Protection;
- ☐ Bring Your Own Device; and
- ☐ PSHCE(E).

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

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

2. Scope of this Policy

This policy applies to all members of the School community, including staff, pupils, parents and visitors, who have access to and are users of the School IT systems – it does not apply specifically to the Seckford Foundation systems except where these are used in the School Context. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the School, including occasional volunteers

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

3. Roles and responsibilities

3.1 The School Committee

The School Committee is responsible for the approval of this policy and for reviewing its effectiveness. The School Committee will review this policy at least annually.

There is a nominated governor responsible for liaison with the DSL and Head of Online Safety.

3.2 Head and the Senior Leadership Team

The Head is responsible for the safety of the members of the School community and this includes responsibility for Online Safety. The Head has delegated day-to-day responsibility to the Head of Online Safety reporting directly to the Designated Safeguarding Lead. In line with KCSIE the DSL has overall responsibility for safeguarding children, including online.

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

- staff, in particular the Head of Online Safety are adequately trained about Online Safety;

and

- staff are aware of the School procedures and policies that should be followed in the event of the abuse or suspected breach of Online Safety in connection to the School.

3.3 Head of Online Safety

The School's Head of Online Safety is responsible to the DSL for the day to day issues relating to Online Safety. The Head of Online Safety has responsibility for ensuring this policy is upheld by all members of the School community and works with IT staff to achieve this. They will keep up to date on current Online Safety issues and guidance issued by the Department for Education: specifically the document "Teaching online safety in school" (June 2019) and the guidance from the UK Council for Child Internet Safety (UKCCIS) "Education for a Connected World" referred to in "Teaching online safety in school", but also by relevant organisations, including, the Suffolk Safeguarding Partnership, CEOP (Child Exploitation and Online Protection), and Childnet International. In addition, we recognise that pupils are likely to be the first to recognise potential risks and are fully consulted in the creation and evaluation of this policy.

3.4 IT staff

The School's technical staff has a key role in maintaining a safe technical infrastructure at the School and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the School's hardware system, its data and for training the School's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and will immediately report inappropriate usage to the Head of Online Safety who, in conjunction with the DSL, checks what is being done. The Head of Online Safety and DSL have access to the monitoring and reporting system.

3.5 Teaching and support staff

As with all issues of safety at this School, staff are encouraged to create a talking and listening culture in order to address any Online Safety issues which may arise in classrooms on a daily basis. **This includes the safeguarding considerations surrounding on-line lessons.**

3.6 Pupils

Pupils are responsible for using the School IT systems in accordance with the Acceptable Use Policy, and for letting staff know if they see IT systems being misused.

3.7 Parents and carers

The School believes that it is essential for parents to be fully involved with promoting Online Safety both in and outside of School. We regularly consult and discuss Online Safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The School will

always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the School.

Parents and carers are responsible for endorsing the School's Pupil Acceptable Use Policy.

4. Education and training

4.1 Staff: awareness and training

New staff receive information on the School's Online Safety and Acceptable Use policies as part of their induction.

All teaching staff receive regular information and training on Online Safety issues in the form of INSET training, training courses and webinars on the National College CPD site, and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of Online Safety.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following School Online Safety procedures. These behaviours are summarised in the Acceptable Use Policy which must be signed and returned before use of technologies in School. When children use School computers, staff should make sure children are fully aware of the agreement they are making to follow the School's IT guidelines.

Teaching staff are encouraged to incorporate Online Safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the School community.

A record of concern must be completed by staff as soon as possible if any incident relating to Online Safety occurs and be provided directly to the School's Head of Online Safety and Safeguarding Lead.

4.2 Pupils: Online Safety in the curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for Online Safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote Online Safety and regularly monitor and assess our pupils' understanding of it.

The School provides opportunities to teach about Online Safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside School will also be carried out via PSHCE(E)), by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, and usually via PSHCE(E), pupils are taught about their Online Safety responsibilities and to look after their own online safety. Pupils are formally taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the Safeguarding Lead, the Head of Online Safety and any member of staff at the School, Woodbridge School Prep or Woodbridge School Pre-Prep.

From Year 1, pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the School's Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the School discovers cases of bullying). Pupils should approach the DSL, Head of Online Safety as well as parents, peers and other School staff for advice or help if they experience problems when using the internet and related technologies.

Online Safety information is also provided to pupils at the School via the VLE Itslearning as news items and on the Online Safety (e-safety) Itslearning mini-site.

4.3 Parents

The School seeks to work closely with parents and guardians in promoting a culture of Online Safety. The School will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the School.

The School recognises that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home. The School therefore arranges annual discussion evenings at Woodbridge School Prep for parents when an outside specialist advises about Online Safety and the practical steps that parents can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm and curiosity.

5. ANTI-CYBERBULLYING

5.1 Policy

Bullying is a most unpleasant aspect of life in any society and at the School we regard it as most important to have a clear policy to prevent it. This is a policy declared by the School and made openly available via the website to staff, pupils and parents so that all parties are committed to upholding it. It should be read in conjunction with the School's Anti-Bullying policy. This policy is applicable to all children, including those in the Early Years Foundation Stage.

It is important to note that with technology and its uses developing rapidly, this document will need to be under fairly constant review and will need to be consulted frequently to keep up to date.

From DfE Preventing and Tackling Bullying:

What is Bullying?

Bullying is behaviour by an individual or group, repeated over time, that intentionally hurts another individual or group either physically or emotionally. Bullying can take many forms (for instance, cyber-bullying via text messages, social media or gaming, which can include the use of images and video) and is often motivated by prejudice against particular groups, for example on grounds of race, religion, gender, sexual orientation, special educational needs or disabilities, or because a child is adopted, in care or has caring responsibilities. It might be motivated by actual differences between children, or perceived differences.

Stopping violence and ensuring immediate physical safety is obviously a school's first priority but emotional bullying can be more damaging than physical; teachers and schools have to make their own judgements about each specific case.

Many experts say that bullying involves an imbalance of power between the perpetrator and the victim. This could involve perpetrators of bullying having control over the relationship which makes it difficult for those they bully to defend themselves. The imbalance of power can manifest itself in several ways, it may be physical, psychological (knowing what upsets someone), derive from an intellectual imbalance, or by having access to the support of a group, or the capacity to socially isolate. It can result in the intimidation of a person or persons through the threat of violence or by isolating them either physically or online.

Low-level disruption and the use of offensive language can in itself have a significant impact on its target. If left unchallenged or dismissed as banter or horseplay it can also lead to reluctance to

report other behaviour. Early intervention can help to set clear expectations of the behaviour that is and isn't acceptable and help stop negative behaviours escalating.

The effect

Bullying can cause its victim anything from short term unhappiness and anxiety to psychological damage. Peer on peer abuse is never tolerated or passed off as "banter" or "part of growing up." In extreme cases bullying has been linked directly to victim suicide. Whilst bullying is not in itself a criminal offence, there are criminal laws which relate to harassment and threatening behaviour. The seriousness of bullying in causing psychological damage and even suicide must never be ignored.

Bullying can happen anywhere and at any time and can involve anyone – pupils, other young people, staff and parents.

5.2 Definition of Cyberbullying

From DfE Preventing and Tackling Bullying:

Cyberbullying

The rapid development of, and widespread access to, technology has provided a new medium for

'virtual' bullying, which can occur in or outside School. Cyberbullying is a different form of bullying which can happen 24/7, with a potentially bigger audience, and more accessories as people forward on content at a click.

Cyberbullying is the sending or posting of harmful or cruel texts or images using the internet or other (digital) communication devices.

There are many different types of cyberbullying:

- Text messages - unwelcome texts that are threatening or cause discomfort.
- Picture/video-clips via mobile phone cameras - images sent to others to make the victim feel threatened or embarrassed.
- Mobile phone calls - silent calls or abusive messages; or stealing the victim's phone and using it to harass others, to make them believe the victim is responsible.
- Emails - threatening or bullying emails, often sent using a made-up name or someone else's name.
- Chatroom bullying - menacing or upsetting replies to children or young people when they are in a web-based chatroom.
- Instant messaging - unpleasant messages sent whilst children are having real time conversations online.

- Bullying via websites - use of blogs (web logs), personal websites and online personal polling sites to spread upsetting lies about someone. This includes social networking websites such as Facebook, Twitter, Tumblr, Instagram etc.

It is important to note that many aspects of cyberbullying outlined above are illegal under UK law, and the School has the right to read e-mail and other electronic communications and take action as a result of information obtained in this way.

The School's view on cyberbullying is that the School will take action to prevent cyberbullying wherever possible and take action to stop such bullying as does occur, whenever the School is involved however peripherally.

5.3 Policy Aims

- To ensure that there is a clear procedure to follow which deals with incidents of cyberbullying and that this is made explicit to staff, pupils and parents.
- To prevent cyberbullying by providing opportunity for discussion by pupils and staff within the School's programme of pastoral care.
- To ensure that all pupils have access to an adult in School to whom they may talk in confidence in the knowledge that something will be done immediately to redress the problem and that the matter will be handled discreetly and sensitively.
- To make the unacceptable nature of cyberbullying and the consequences of any repetition clear to the cyberbully and his/her parents/guardians.
- To follow up each incident so as to ensure that the victim is given as much support as possible and also to prevent a recurrence of the behaviour.
- To make clear to parents of both victims and cyberbullies the actions which are being taken by the School, the reasons for doing so and the extent of the support which parents can offer to reinforce those actions.

5.4 Shared information, discussion and co-operation between teachers and parents

- Parents play an essential role in the education of their children and in the monitoring regulation of the children's on-line behaviours.
- Through Itslearning (for staff and pupils) and via pages on the School's website (for parents and others), online safety information is shared as appropriate.
- The School provides information and awareness to parents through seminars and other methods as appropriate.

5.5 Procedure - Senior School

- Any incident of cyberbullying must be reported to the pupil's Tutor, the School's Head of Online Safety, a Head of House, Head or Lower School (or deputy), Director of Sixth Form (or deputy) Head of Boarding, or Deputy Head (Pastoral). Incidents may be reported via any member of staff (whether teaching, administrative or support), prefects, pupils or parents/guardians. The Tutor/online safety officer/Housemaster/Mistress etc. will report the incident to the Deputy Head (Pastoral). Investigation may be undertaken by the online safety officer, and/or the Network Manager and staff.
- The DSL will also be informed to check there are no safeguarding implications.
- When it is deemed necessary, by the Deputy Head (Pastoral), written accounts will be required from all those involved.
- Sanctions to be applied as appropriate include: suspension of an individual's internet access at School and/or suspension of an individual's user account for a period of time.
- In serious cases (and where cyberbullying by an individual continues) the Head may decide to exclude from School the person or persons responsible.
- Through regular communication between the online safety officer and Deputy Head (Pastoral), Director of Sixth Form, Housemasters/Mistresses, Head of Lower School, Head of Boarding, Tutors, and Pupil Support Group, it is hoped that any pupil who either seems to be a victim of cyberbullying or is repeatedly being a cyberbully will be quickly identified.

5.6 Procedure - Woodbridge School Prep

- Any incident of cyberbullying must be reported to the pupil's class teacher and the Head of Woodbridge School Prep. Incidents may be reported via any member of staff (whether teaching, administrative or support), pupils or parents/guardians. Investigation may be undertaken by Woodbridge School Prep Teacher responsible for computing and/or the Network Manager and staff. The online safety officer must be informed of the incident if not included in the investigation.
- The DSL will also be informed if there are deemed safeguarding implications.
- When it is deemed necessary, by the Head, written accounts will be required from all those involved. The Head will contact the parents of those pupils involved.
- Sanctions to be applied as appropriate include: suspension of an individual's internet access at School.
- In serious cases (and where cyberbullying by an individual continues) the Head, in may decide to exclude from School the person or persons responsible.
- Through regular communication between the class teachers, the Deputy Head or the Head, it is hoped that any pupil who either seems to be a victim of cyberbullying or is repeatedly being a cyberbully will be quickly identified.

5.7 Further resources:

Specialist Organisations:

- E-safer Suffolk: www.esafersuffolk.org which offers lots of support and strategies, and has amongst other information a comprehensive list of other sites to explore: http://www.suffolk.gov.uk/your-community/e-safer-suffolk/online safety-tips-and- advice#A1
- Anti-bullying Alliance (ABA): Brings together more than 65 organisations with the aim of reducing bullying and creating safer environments in which pupils can live, grow, play and learn.
- Beatbullying: Beatbullying is the leading bullying prevention charity in the UK and provides anti-bullying resources, information, advice and support for young people, parents and professionals affected by bullying.
- Kidscape: Kidscape is a charity working UK-wide to keep children safe from bullying and sexual abuse.
- Childnet International: Specialist resources for young people to raise awareness of online safety and how to protect themselves.
- Child Exploitation and Online Protection Centre: www.ceop.police.uk. The Child Exploitation and Online Protection (CEOP) Centre is dedicated to eradicating the sexual abuse of children. That means we are part of UK policing and very much about tracking and bringing offenders to account either directly or in partnership with local and international forces.

5.8 References:

- DfE Preventing and Tackling Bullying: Preventing and tackling bullying
- DfE: Supporting children and young people who are bullied: advice for Schools
- DfE Keeping Children safe in Education
- DfE Searching, Screening and Confiscation

6. E-MAIL AND INTERNET

6.1 Policy statement

The School provides access to the internet and e-mail provision. This access is intended to be used for work purposes only and the School endeavours to maintain a safe and appropriate online environment for both staff and pupils.

Internet access is provided for members of the boarding house via Wi-Fi in the evenings until 11pm. This access is provided for both work and leisure purposes and is also filtered and monitored.

6.2 Staff

Staff must not access social networking sites/personal email whilst teaching / in front of pupils unless such use is necessary for the purposes of education (for the teaching of PHSCE(E), for example). Such access may only be made from staff member's own devices whilst in staff-only areas of School or when not teaching.

When accessed from staff member's own devices / off School premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the School.

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

Staff must immediately report to the Head of Online Safety and IT Manager or their line manager the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the Head of Online Safety / IT Manager and Head of Finance.

Any online communications must not either knowingly or recklessly:

- ☐ place a child or young person at risk of harm, or cause actual harm;
- ☐ bring the School into disrepute;
- ☐ breach confidentiality;
- ☐ breach copyright;

☐ breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:

- o making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
- o using social media to bully another individual; or
- o posting links to or endorsing material which is discriminatory or offensive.

Under no circumstances should School pupils be added or accepted as social network 'friends' or contacted through social media until the pupil is at least 21 years of age.

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer using the staff member's personal email address. The School ensures that staff have access to their work email address when offsite, for use as necessary on School business.

6.3 Pupils

All pupils are issued with their own personal School email addresses for use on our network-. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure and must be used for all School work including assignments / research / projects. Pupils should be aware that email communications through the School network and School email addresses are monitored.

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

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication to the Head of Online Safety / Deputy Head (Pastoral) or their tutor in the first instance.

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

Pupils must report any accidental access to materials of a violent or sexual nature directly to the Head of Online Safety / Designated Safeguarding Lead. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under

the School's Behaviour Management Policy. Pupils are aware that all internet usage via the School's systems and its wifi network is monitored.

Certain websites are automatically blocked by the School's filtering system. If this causes problems for School work / research purposes, pupils should contact IT team for assistance.

6.4 Data storage and processing

The School takes its compliance with the Data Protection Act 1998 seriously. Please refer to the Data Protection Policy and the Acceptable Use Policy for further details.

Staff and pupils are expected to save all data relating to their work to their School laptop / PC or to the School's central server.

Staff devices should be encrypted if any data or passwords are stored on them.

Staff may only access information offsite when authorised to do so, such as using iSAMS for School-related work, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by the School or online encrypted storage such as the School-provided OneDrive.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Head of Online Safety and IT staff.

6.5 Password security

Pupils and staff have individual School network logins, email addresses and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should:

- ☐ use a strong password (containing eight characters or more and containing upper and lower case letters as well as numbers).
- ☐ not write passwords down; and
- ☐ not share passwords with other pupils or staff.

6.6 Safe use of digital and video images

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

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

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

Staff and volunteers are allowed to take digital / video images to support educational aims but must follow this policy [and the Acceptable Use Policy / IT Policy / EYFS Policy] concerning the sharing, distribution and publication of those images. Those images should only be taken on School equipment: personal equipment should not be used for such purposes.

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

Pupils must not take, use, share, publish or distribute images of others, even with their permission.

The School will undertake monitoring or examination of pupil's accounts and devices where appropriate to enforce this rule in line with DfE guidance 'Searching, Screening and Confiscation (January 2018)

Photographs published on the School website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images.

6.7 Misuse

The School will not tolerate illegal activities or activities that are inappropriate in a School context and will report illegal activity to the police and/or the Suffolk Safeguarding Children Board (SSCB). If the School discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the Child Exploitation and Online Protection Centre (CEOP).

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the School's policies and procedures (in particular the Safeguarding Policy) / the Online Safety process incident flowchart.

The School will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policy.

6.8 Complaints

As with all issues of safety at The School, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to Online Safety prompt action will be taken to deal with it. Complaints should be addressed to the Head of Online Safety or to the Designated Safeguarding Lead in the first instance, who will liaise with the leadership team who will undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of or concerns around Online Safety will be recorded using a Record of Concern form and reported to the School's Head of Online Safety and the Designated Safeguarding Lead, Ben Capjon, in accordance with the School's Child Protection Policy.

6.9 Bring Your Own Device (BYOD)

- Users who connect their own devices to the School's network are bound by the School's policies.
- The School adheres to the principles of the Data Protection Act.
- All users are provided with and accept the relevant AUP agreement.
- All School network systems are secure and the wireless network is configured to require logins so that users can be identified and different policies by category can be applied, as on the cabled network.
- Devices connected to the School's network are covered by the School's normal filtering systems.

- Users accessing the School's wireless networks are required to log on. Connection of a user's device to the School's network is recorded.
- Pupils receive guidance on the use of personal devices.

7. BRING YOUR OWN DEVICE (BYOD) POLICY FOR STAFF AND VISITORS

7.1 Introduction

The School recognises that mobile technology offers valuable benefits to staff 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 members 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. If you are unsure whether your device is captured by this policy, please check with the School's Head of Online Safety. 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.

This policy is supported by the Staff Acceptable Use Policy.

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.

7.2 Policy statements

7.3 Use of mobile devices at the School

Staff and visitors to the School may use their own mobile devices in the following locations:

☐ In the classroom with the permission of the teacher

☐ In the School environs.

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.

While the School provides devices listed above to a limited extent, it is inevitable that staff will want (or need, on occasions) to use their own personal devices for these purposes and given the scale of use it is not appropriate or even realistic to expect that this can be avoided, apart from in the EYFS setting in which different conditions apply. For the policy on mobile technologies in the EYFS setting, please see the School Safeguarding policy.

With this in mind, it is expected that staff will only use equipment provided by or authorised by the School. In the case of mobile telephones and tablet devices, it is expected that a personal device will only be used outside the EYFS setting, and only when a School-provided device is unavailable, and staff should have authorisation from the Designated Safeguarding Lead to do so.

7.4 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 pupils other than their own in photographs, video, or audio, and other visitors and staff should 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 policy and anti-bullying policy when making photographs, videos, or audio recordings.

7.5 Access to the School's internet connection

The School provides a wireless network that staff 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.

The School cannot guarantee that the wireless network is secure, and staff and visitors use it at their own risk. In particular, staff and visitors are advised not to use the wireless network for online banking or shopping.

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.

7.6 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;

☐ the School virtual learning environment;

☐ iSAMS.

☐ Remote desktop and office facilities where provided

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 or HR department as soon as possible.

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. Users must follow the written procedures for connecting to the School systems.

7.7 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, 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 Head of Online Safety and IT team as soon as possible.

7.8 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 online 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.

7.9 Compliance with Data Protection Policy

Staff compliance with this BYOD policy is an important part of the School's compliance with the Data Protection Act 2018 and GDPR. Staff must apply this BYOD policy consistently with the School's Data Protection Policy.

7.10 Support

The School takes no responsibility for supporting staff's own devices; nor has the School a responsibility for conducting annual PAT testing of personally-owned devices.

7.11 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 in accordance with its disciplinary policy. 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.

7.12 Incidents and Response

The School takes any security incident involving a staff member's or visitors 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 Chief Executive's office.

8. BRING YOUR OWN DEVICE (BYOD) POLICY FOR PUPILS

8.1 Introduction

The School recognises that mobile technology offers valuable benefits to staff 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 pupils of 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. If you are unsure whether your device is captured by this policy, please check with the School's Head of Online Safety. These devices are referred to as 'mobile devices' in this policy.

This policy is supported by the Acceptable Use Policy.

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.

8.2 Policy statements

See below:

8.3 Use of mobile devices at the Senior School

Pupils in Years 7 – 11 may use their own mobile devices:

- In the classroom with the permission of the teacher for educational purposes only
- In the valley and gravel quad at lunch and break time. This is currently (2021-22) being *trialled* and subject to review.

- In the classroom with the permission of the teacher for educational purposes only

- In the Sixth Form Common Room

Pupils 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. The School Office must be notified immediately of any damage, loss, or theft of a mobile device, and these incidents will be logged.

Mobile devices must not be taken into controlled assessments and/or examinations, unless special circumstances apply. Boarders in Years 9 and 10 are required to hand in their phones before bedtime.

The School reserves the right to refuse pupils permission to use their own mobile devices on School premises.

The School reserves the right to immediately confiscate a mobile device from any pupil who contravenes any of the above. The mobile device should be handed in to the reception in an envelope with the pupil's name and should only be returned after 4.10p.m.

8.4 Use of electronic devices at the Prep School

Pupils are not to bring mobile devices to School unless they travel on School buses or by public transport. Parents of pupils who do carry mobile devices on their journeys are to write to The Head for permission and mobile devices are to be handed into Matron for safekeeping during the School day.

On some residential School trips pupils will be allowed to carry mobile devices, but this will be decided by the member of staff organizing the trip.

Mobile devices should never be used to take photographs or video of other pupils.

The School reserves the right to immediately confiscate a mobile device from any pupil who contravenes any of the above. The mobile device should be handed to the Head of Woodbridge School Prep in an envelope with the pupil's name on it. Any contravention of the policy on photography will be treated extremely seriously.

The School is not responsible for the investigation of any incident of a mobile device being stolen, lost or damaged, either wilfully or accidentally. Pupils entrusted with a mobile device should also acknowledge their responsibility for its security. Neither will the School be responsible for any misuse of a mobile device by another pupil.

Pupils may be provided with electronic devices by the School for educational purposes (for ipads and laptops).

Pupils in Years 5 and 6 are invited to participate in the BYOD scheme for educational purposes. Acceptable devices include laptops and tablets with Windows compatibility. All pupils and parents must sign the Acceptable Use Policy to ensure they understand the requirements and expectations.

8.5 Use of cameras and audio recording equipment

Pupils may not use cameras or recording equipment to take photographs or video of staff members without explicit, individual permission, and it should be assumed that this permission will NOT be given except under very specialised circumstances.

Pupils may not take photographs or videos of other pupils even with the pupil's permission.

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. Pupils must comply with the School's social media policy and anti-bullying policy when making photographs, videos, or audio recordings.

8.6 Access to the School's internet connection

The School provides a wireless network that 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.

The School cannot guarantee that the wireless network is secure, and pupils use it at their own risk. 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.

8.7 Access to School IT services

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

- the School email system;

- the School virtual learning environment;

Pupils must only use the IT services listed above and any information accessed through them for work purposes. Pupils 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 or Head of Online Safety as soon as possible.

Pupils must not send School information apart from homework 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. Users must follow the written procedures for connecting to the School systems.

8.8 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, pupils 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, 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.

Pupils who receive any inappropriate content through School IT services or the School internet connection should report this to the Head of Online Safety as soon as possible.

8.9 Security of pupil mobile devices

Pupils 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.

Pupils must never attempt to bypass any security controls in School systems or others' own devices. Pupils are reminded to familiarise themselves with the School's online-safety, social media and

acceptable use of IT policies which set out in further detail the measures needed to ensure

responsible behaviour online.

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

8.10 Support

The School takes no responsibility for supporting pupil's own devices; nor has the School a responsibility for conducting annual PAT testing of personally owned devices

8.11 Additional comments relating to Woodbridge School Prep

BYOD Agreement Woodbridge School Prep (Years 5 & 6) (Pupils and parents to sign)

I understand that I must ensure that:

Malware protection is fully installed on the electronic device

I abide by the rules outlined in the policy

I do not record or share any clips, audio or visual of pupils or staff

I will not attempt to share or show any information, images, video or audio with peers, other than that authorised by staff as educational

I understand that failure to adhere to these rules will result in the privilege of BYOD being revoked and possible denial of access to school computer systems.

All usual rules regarding online safety and behaviour remain in addition to this agreement.

Signed Pupil:

Signed Parent/ Guardian:

Date:

9. USE OF PERSONAL IMAGES

9.1 POLICY

9.2

This Policy

This Policy is intended to provide information to pupils and their parents, carers or guardians (referred to in this policy as "parents") about how images of pupils are normally used by Woodbridge School ("the School"). It also covers the School's approach to the use of cameras and filming equipment at School events and on School premises by parents and pupils themselves, and the media.

It applies in addition to the School's parent contract, and any other information the

School may provide about a particular use of pupil images, including e.g. signage about the use of CCTV; and more general information about use of pupils' personal data, e.g. the School's Privacy Notice. Images of pupils in a safeguarding context are dealt with under the School's relevant safeguarding policies.

9.3 General points to be aware of

Certain uses of images are necessary for the ordinary running of the School; other uses are in the legitimate interests of the School and its community and unlikely to cause any negative impact on children. The School is entitled lawfully to process such images and take decisions about how to use them, subject to any reasonable objections raised.

Consent is given via signing the parental contract to the School indicating agreement to the school using images of pupils as set out in this policy. The parent should contact the School if this becomes unacceptable. However, parents should be aware of the fact that certain uses of their child's images may be necessary or unavoidable (for example if they are included incidentally in CCTV or a photograph).

We hope parents will feel able to support the School in using pupil images to celebrate the achievements of pupils, sporting and academic; to promote the work of the School; and for important administrative purposes such as identification and security.

Any parent who wishes to limit the use of images of a pupil for whom they are responsible should contact the Head's PA in writing. The School will respect the wishes of parents/carers (and indeed pupils themselves) wherever reasonably possible, and in accordance with this policy.

Parents should be aware that, from around the age of 12 and upwards, the law recognises pupils' own rights to have a say in how their personal information is used – including images.

9.4 Use of Pupil Images in School Publications

Unless the relevant pupil or his or her parent has requested otherwise, the School will use images of its pupils to keep the School community updated on the activities of the School, and for marketing and promotional purposes, including:

- on internal displays (including clips of moving images) on digital and conventional notice boards within the School premises;
- in communications with the School community (parents, pupils, staff, Governors and alumni) including by email, on the School intranet and by post;
- on the School's website and, where appropriate, via the School's social media channels, e.g. Twitter, Instagram and Facebook and in the School's prospectus, and in online, press and other external advertisements for the School.
- The source of these images will predominantly be the School's staff (who are subject to policies and rules in how and when to take such images), or a professional photographer used for marketing and promotional purposes, or occasionally pupils. The School will only use images of pupils in suitable dress and the images will be stored securely and centrally.

9.5 Use of Pupil Images for Identification and Security

All pupils are photographed on entering the School and, thereafter, at annual intervals, for the purposes of internal identification. These photographs identify the pupil by name, year group, house and form/tutor group.

CCTV is in use on School premises and will sometimes capture images of pupils.

Images captured on the School's CCTV system are used in accordance with the Privacy Notice and CCTV Policy / any other information or policies concerning CCTV which may be published by the School from time to time.

9.6 Use of Pupil Images in the Media

Where practicably possible, the School will always notify parents in advance when the media is expected to attend an event or School activity in which School pupils are participating, and will make every reasonable effort to ensure that any pupil whose parent or carer has refused permission for images of that pupil, or themselves, to be made in these circumstances are not photographed or filmed by the media, nor such images provided for media purposes.

The media often asks for the names of the relevant pupils to go alongside the images, and names will only be provided where parents have been informed about the media's visit and consented as appropriate.

9.7 Security of Pupil Images

Professional photographers and the media are accompanied at all times by a member of staff when on School premises. The School uses only reputable professional photographers and makes every effort to ensure that any images of pupils are held by them securely, responsibly and in accordance with the School's instructions.

The School takes appropriate technical and organisational security measures to ensure that images of pupils held by the School are kept securely on School systems and protected from loss or misuse. The School will take reasonable steps to ensure that members of staff only have access to images of pupils held by the School where it is necessary for them to do so.

All staff are given guidance on the School's Policy on Taking, Storing and Using Images of Pupils, and on the importance of ensuring that images of pupils are made and used responsibly, only for School purposes, and in accordance with School policies and the law.

9.8 Use of Cameras and Filming Equipment (including mobile phones) by Parents

Parents, guardians or close family members (hereafter, parents) are welcome to take photographs of (and where appropriate, film) their own children taking part in School events, subject to the following guidelines, which the School expects all parents to follow:

- When an event is held indoors, such as a play or a concert, parents should be mindful of the need to use their cameras and filming devices with consideration and courtesy for cast members or performers on stage and the comfort of others. Flash photography can disturb others in the audience, or even cause distress for those with medical conditions; the School therefore asks that it is not used at indoor events.
- Parents are asked not to take photographs of other pupils, except incidentally as part of a group shot, without the prior agreement of that pupil's parents.
- Parents are reminded that such images are for personal use only. Images which may, expressly or not, identify other pupils should not be made accessible to others via the internet (for example on Facebook), or published in any other way.
- Parents are reminded that copyright issues may prevent the School from permitting the filming or recording of some plays and concerts. The School will always print a reminder in the programme of events where issues of copyright apply.

- Parents may not film or take photographs in changing rooms or backstage during School productions, nor in any other circumstances in which photography or filming may embarrass or upset pupils.
- The School reserves the right to refuse or withdraw permission to film or take photographs (at a specific event or more generally), from any parent who does not follow these guidelines, or is otherwise reasonably felt to be making inappropriate images.
- The School sometimes records plays and concerts professionally (or engages a professional photographer or film company to do so), in which case CD, DVD or digital copies may be made available to parents for purchase. Parents of pupils taking part in such plays and concerts will be consulted if it is intended to make such recordings available more widely.

9.9 Use of Cameras and Filming Equipment by Pupils

- All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology, or any worrying issues to a member of the pastoral staff.
- The use of cameras or filming equipment (including on mobile phones) is not allowed. Exceptions may be made to this for work in photography, but this will be with the express

permission of staff. Nor should photography or filming equipment be used by pupils in a manner that may offend or cause upset.

- The misuse of images, cameras or filming equipment in a way that breaches this Policy, or the School's Anti-Bullying Policy, Data Protection Policy (Staff and Pupils), IT Acceptable Use Policy for Pupils (see appendicles to this policy), Safeguarding Policy or the School Rules is always taken seriously, and may be the subject of disciplinary procedures or dealt with under the relevant safeguarding policy as appropriate.

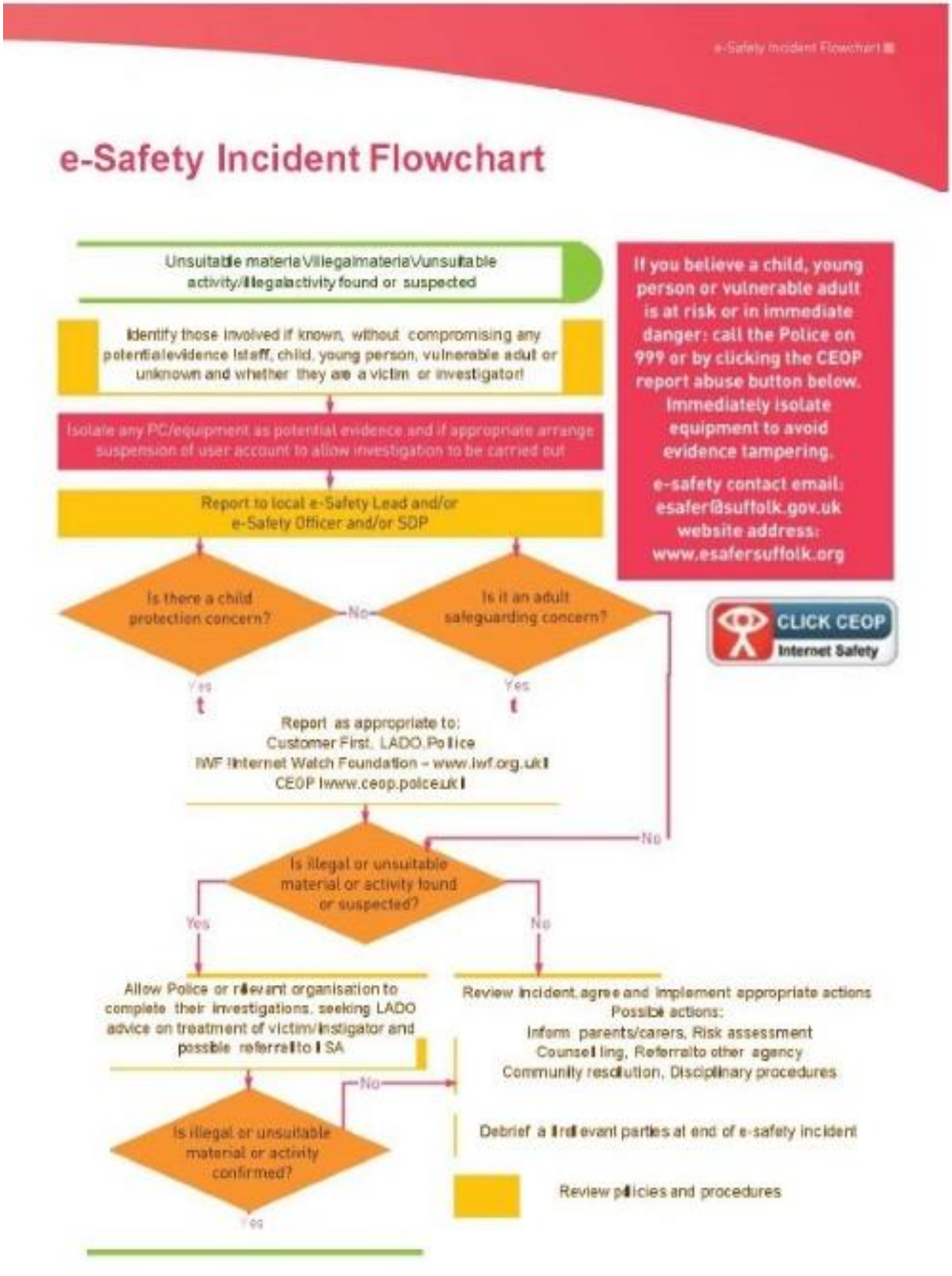
10. Compliance and Monitoring arrangements

This policy will be subject to a thorough review process including consideration at the Education Committee on an annual basis. This will ensure that practice across the whole school is in line with *this* policy, the Complaints procedure and with current guidance and legislation.

Appendix A: Head of Online Safety JOB DESCRIPTION

- Developing an online safety culture under the direction of the management team and acting as a named point of contact on all online safety issues.
- Ensuring that everyone including pupils know what to do if they are concerned about an online safety issue.
- Ensuring that online safety is embedded within continuing professional development (CPD) for staff and co-ordinating training as appropriate.
- Ensuring that online safety is embedded across activities as appropriate.
- Ensuring that online safety is promoted to parents and carers, other users and pupils of ICT resources and supporting them in their understanding of the issues.
- Maintaining an online safety incident log.
- Monitoring and reporting on online safety issues to the management team, and other agencies as appropriate.
- Developing an understanding of the relevant local and national guidance.
- In consultation with the Senior Management Team, liaising with the local authority, Police, IWF, (Internet Watch Foundation www.iwf.org.uk) and CEOP (Child Exploitation and Online Protection Centre www.ceop.police.uk) as appropriate.
- Reviewing and updating online safety policies and procedures on a regular basis and after an incident.
- Ensure that learning outcomes and feedback are appropriately shared.
- Ensuring that the infrastructure and technology provides a safe and secure environment for pupils.

Appendix B


e-Safety Incident Flowchart
Unsuitable material/illegal material/unsuitable activity/illegal activity found or suspected
Identify those involved if known, without compromising any potential evidence (staff, child, young person, vulnerable adult or unknown and whether they are a victim or investigator)
Isolate any PC/equipment as potential evidence and if appropriate arrange suspension of user account to allow investigation to be carried out
Report to local e-Safety Lead and/or e-Safety Officer and/or SDP
Is there a child protection concern?
No
Is it an adult safeguarding concern?
Yes
Yes
Report as appropriate to:
Customer First, LADO, Police
IWF (Internet Watch Foundation – www.iwf.org.uk)
CEOP (www.ceop.police.uk)
No
Is illegal or unsuitable material or activity found or suspected?
Yes
No
Allow Police or relevant organisation to complete their investigations, seeking LADO advice on treatment of victim/instigator and possible referral to ISA
Review incident, agree and implement appropriate actions
Possible actions:
Inform parents/carers, Risk assessment
Counselling, Referral to other agency
Community resolution, Disciplinary procedures
No
Is illegal or unsuitable material or activity confirmed?
Yes
Debrief all relevant parties at end of e-safety incident
Review policies and procedures
If you believe a child, young person or vulnerable adult is at risk or in immediate danger: call the Police on 999 or by clicking the CEOP report abuse button below.
Immediately isolate equipment to avoid evidence tampering.
e-safety contact email: esafer@suffolk.gov.uk
website address: www.esafersuffolk.org
CLICK CEOP
Internet Safety

Appendix C

ACCEPTABLE USE POLICY AGREEMENT

Scope of this Policy

This policy applies to all members of the School community, including staff, pupils, parents, and visitors. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the School, including occasional volunteers.

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.
- ☐ 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).
- ☐ 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.
- ☐ 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 pupils or parents, and pupils 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

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 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.

Compliance with related School policies

You will ensure that you comply with the School's Online Safety Policy and other relevant policies in the Online Safety Portfolio.

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 Online 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 Head of Online Safety (Mr Jim Hillman). Reports will be treated in confidence.

Acceptance of this policy

Please confirm that you understand and accept this policy by ticking below and returning the signed copy to the Head of IT. (This will also be confirmed by ticking the on-screen box in the AUP login screen on the network.)

I understand and accept this acceptable use policy.

Appendix D

GLOSSARY OF CURRENT ROLE HOLDERS

The following roles referred to in these policies are currently held by:

Head – Shona Norman

Deputy Head (Pastoral) – Ben Capjon

Designated Safeguarding Lead – Ben Capjon

Head of Online Safety – Jim Hillman

Head of Woodbridge School Prep – Nicola Mitchell

Deputy Head of Woodbridge School Prep – Philippa Martin

Appendix E

Quick Reference Social Media Guidelines

These guidelines are for ALL members of staff about the use of images and names on social media.

- Use first names only (inc when with a picture).
- Consider how important an identifiable image is
- Make sure the image is less identifiable (e.g., group picture with no reference to who, for example John is, or a photo of them conducting the activity from a distance)
- With external media (newspapers etc) full names may be used but only after parents are consulted and have given consent.

EYFS

- No names of pupils for children at Woodbridge School Prep/Woodbridge School Pre-Prep in EYFS years (birth – 5 years old).

If you have any questions, please contact either:

- Designated Safeguarding Lead;
- Director of Operations (also School DPO);
- Woodbridge School Head;
- Woodbridge School Prep and Pre-Prep Head;
- Woodbridge School Prep Deputy Head;
- Head of Online Safety;
- Marketing.

Appendix F

BYOD September 2020

E-Safety Checklist for Parents

	Pupils in Years 5 and 6 are invited to BYOD in order to maintain the digital literacy skills learned in lockdown that pupils will need. This is expedient given the potential for further periods of remote learning in our current, uncertain times. Since March, many families have invested in devices for School use; others may be thinking of doing so in the near future. This guide aims to give parents a helpful checklist of E-Safety considerations and actions. Year 5 - BYOD Friday Year 6 - BYOD Tuesday (A device = laptop or tablet: Windows compatible) At Woodbridge School Prep, we value a hands-on, creative, unplugged School Day where computers are a tool to be mastered. Devices will only be used to access lesson resources, via the itslearning platform, as directed by teachers.	