

# **Online Safety Policy (including Online Safety Acceptable Use Agreement)**

<b>Start Date:</b>	<b>Spring 2024</b>
<b>Date of Next Review:</b>	<b>Spring 2026</b>
<b>Author:</b>	<b>Mrs M Goodes</b>
<b>Responsible Committee:</b>	<b>Education Committee</b>

# Contents

1. Introduction.....	1
2. Responsibilities .....	1
3. Scope of policy .....	1
4. Policy and procedure.....	2
Use of email .....	2
Visiting online sites and downloading .....	2
Storage of Images .....	4
Use of personal mobile devices (including phones) .....	4
Reporting incidents, abuse and inappropriate material.....	5
5. Curriculum .....	5
6. Staff and Governor Training.....	6
7. Working in Partnership with Parents/Carers .....	6
8. Records, monitoring and review .....	7
9. Appendices of the Online Safety Policy.....	7
A. Online Safety Acceptable Use Agreement - Staff, Governors and student teachers (on placement or on staff) .....	7
B. Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers .....	7
Appendix A - Online Safety Acceptable Use Agreement - Staff, Governors and student teachers (on placement or on staff).....	8
Appendix B - Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers ....	11
Appendix C - Requirements for visitors, volunteers and parent/carers helpers .....	14
Appendix D - Online Safety Acceptable Use Agreement: Students.....	15
Appendix E - Online safety policy guide - Summary of key parent/carers responsibilities .....	17
Appendix F - Guidance on the process for responding to cyberbullying incidents .....	18
Appendix G - Guidance for staff on preventing and responding to negative comments on social media .....	19
Appendix H – Links to the relevant GDPR Policy .....	20

## 1. Introduction

Haileybury Turnford school recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all** students, staff, and governors will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some students may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

## 2. Responsibilities

The principal and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named online safety lead in this school is **Maxine Goodes**

All breaches of this policy must be reported to **the Online Safety Lead**.

All breaches of this policy that may have put a child at risk must also be reported to the DSL (Designated Safeguarding Lead), **the Online Safety Lead**.

Organisations that are renting space from the school and are a separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network, cloud-based services and/or equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

If the organisation is operating in school time or when students are on site in the care of the school, then the safeguarding of students is paramount, and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

## 3. Scope of policy

The policy applies to:

- students
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

The school also works with partners and other providers to ensure that students who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, for example, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe

online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents: safeguarding, Keeping Children Safe in Education, GDPR (General Data Protection Regulations) Appendix H, health and safety, home–school agreement, home learning, rewards, discipline and behaviour, anti-bullying and PSD/RSE policies.

#### 4. Policy and procedure

The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for students, parents/carers, staff and governors and all other visitors to the school.

##### Use of email

Staff should use a school email account or Governor Hub for all official school communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact students, parents or conduct any school business using a personal email address. Students should use school approved accounts on the school system for educational purposes. Where required parent/carer permission will be obtained for the student account to exist. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the policies for GDPR. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff, governors, and students should not open emails or attachments from suspect sources and should report their receipt to **the Online Safety Lead**.

**Users must not** send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

##### Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in school or before recommending them to students. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service and seek approval from a senior leader. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required. If internet research is set for homework, specific sites will be suggested that have been checked by the teacher. All users must observe copyright of materials from electronic sources.
- Staff must only use pre-approved systems if creating blogs, wikis or other online content.
- When working with students searching for images should be done through Google Safe Search (standard through the schools' broadband system).

**Users must not:**

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
- Adult material that breaches the Obscene Publications Act in the UK
- Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation
- Promoting hatred against any individual or group from the protected characteristics above
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

**Users must not:**

- Reveal or publicise confidential or proprietary information
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school
- Use the school's hardware and Wi-Fi facilities for running a personal business
- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the school

School devices may be used to conduct school business outside of school. Personal devices may be used to conduct school business by utilising one of the approved mechanisms that connect via the RDS server (Remote Desktop Services). This is a closed, monitorable system designed specifically for this purpose. Using this system users are unable to save files locally to their own device, thereby breaching data security

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by **the Online Safety Lead**.

### Storage of Images

Photographs and videos provide valuable evidence of students' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See GDPR Data Protection Policy 27-09-2021.pdf for greater clarification).

Photographs and images of students are only stored on the school's agreed secure networks which include some cloud-based services. Rights of access to stored images are restricted to approved staff as determined by **the Online Safety Lead**. Staff and students may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons' parents/carers must follow the school's Acceptable Use Agreement (Appendix E) and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with students, must only use school equipment to record images of students whether on or off site. Permission to use images of all staff who work at the school is sought on induction and a written record is in the personnel file.

### Use of personal mobile devices (including phones)

The school allows staff, including temporary and peripatetic staff, to use personal mobile phones and devices for school related business only as necessary. Under no circumstance does the school allow a member of staff to contact a student or parent/carer using their personal device.

Parents/carers may only use personal mobile phones and devices unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child unless there is a pre-specified permission from the Online Safety Lead. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

Students are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes during the school day. During the school day all such devices must be switched off and out of sight. Under no circumstance should students use their personal mobile devices/phones to take images of

- any other student unless they and their parents have given agreement in advance and not during the school day.
- any member of staff

The school is not responsible for the loss, damage or theft of any personal mobile device

that is brought into school.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Personal devices may be used to conduct school business by utilising one of the approved mechanisms that connect via the RDS server (Remote Desktop Services). This is a closed, monitorable system designed specifically for this purpose. Using this system users are unable to save files locally to their own device, thereby breaching data security.

#### New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefit and carry out risk assessment before use in school is allowed. Parents/carers, students and staff should not assume that new technological devices will be allowed in school and should check consult with the Network Manager and Online Safety Lead before approving new technological devices before they are brought into school.

#### Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a student or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the student or adult must report the incident immediately to the first available member of staff, the DSL, the principal or **Online Safety Lead**. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to social care or the police.

### **5. Curriculum**

Online safety is fully embedded within our curriculum. The school provides a comprehensive age-appropriate curriculum for online safety which enables students to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The PSD curriculum, Relationships and Sex Education Curriculum are central in supporting the delivery of online safety education.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for students to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Students are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity
- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment
- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and

extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives) Understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online

- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others
- Understanding the permanency of all online postings and conversations

Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images.

- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.
- How the law can help protect against online risks and abuse

## **6. Staff and Governor Training**

Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

New staff are provided with a copy of the online safety policy and must sign the school's Acceptable Use Agreement (Appendix A) as part of their induction and before having contact with students.

Any organisation working with children and based on the school premises are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement (Appendix B).

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement (Appendix B).

Guidance is provided for occasional visitors, volunteers, and parent/carers helpers (Appendix C).

## **7. Working in Partnership with Parents/Carers**

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.

It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of recent technologies and associated risks. The school provides regular updated online safety information through the school website, newsletters and by other means.

Parents/carers are asked on an annual basis to read, discuss and co-sign with each



child the Acceptable Use Agreement (Appendix B). A summary of key parent/carer responsibilities will also be provided and is available in Appendix F The Acceptable Use Agreement explains the school's expectations and student and parent/carer responsibilities.

## **8. Records, monitoring and review**

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly to ensure they are effective and that the risks to students and staff are minimised.

All breaches of this policy must be reported, and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported. Incidents are reported and recorded on CPOMS.

The school supports students and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Governors receive termly summary data on recorded online safety incidents for monitoring purposes. In addition, governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.

## **9. Appendices of the Online Safety Policy**

- A. Online Safety Acceptable Use Agreement - Staff, Governors and student teachers (on placement or on staff)
- B. Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers
- C. Requirements for visitors, volunteers and parent/carer helpers working in the school (working directly with children or otherwise)
- D. Online Safety Acceptable Use Agreement - Students
- E. Online safety policy guide - Summary of key parent/carer responsibilities
- F. Guidance on the process for responding to cyberbullying incidents
- G. Guidance for staff on preventing and responding to negative comments on social media

## **Appendix A - Online Safety Acceptable Use Agreement - Staff, Governors and student teachers (on placement or on staff)**

You must read this agreement in conjunction with the online safety policy and the GDPR policies. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life, and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff, student teachers and governors are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with the Online Safety Lead. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply, and police involvement will be sought.

### **Internet Access**

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL and an incident report completed.

### **Online conduct**

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the Online Safety Lead.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, principal and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to students and/or parents/carers.

### **Social networking**

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or students on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or students. This includes contact with former students, considering ex-students who are also known to be 'vulnerable' young people up to the age of 25.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or students. Privileged information must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

### **Passwords**

I understand that there is no occasion when a password should be shared with a student or anyone, including work colleagues.

## **Data protection**

I will follow requirements for data protection as outlined in GDPR policies. These include:

- Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely
- Personal data can only be taken out of school or accessed remotely when authorised by the principal or governing body
- Personal or sensitive data taken off site must be encrypted

## **Images and videos**

I will only upload images or videos of staff, students or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of school events or activities on any personal device.

## **Use of email**

I will use my school email address or governor hub for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my school email addresses or governor hub for personal matters or non-school business.

## **Use of personal devices**

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me because of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the principal.

I will only use approved personal devices in designated areas.

I will not access secure school information from personal devices when in school or any other location unless a closed, monitorable system has been set up by the school. Such a system would ensure as the user I was not saving files locally to my own device and breaching data security.

## **Additional hardware/software**

I will not install any hardware or software on school equipment without permission of the Online Safety Lead.

## **Promoting online safety**

I understand that online safety is the responsibility of all staff and governors, and I will always promote positive online safety messages including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, students or parents/carers) to the DSL or Online Safety Lead.

## **Classroom management of internet access**

I will pre-check for appropriateness all internet sites used in the classroom this will include the acceptability of other material visible, however briefly, on the site. I will not free surf the internet in front of students. I will also check the appropriacy of any suggested sites suggested for home learning.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in

advance for the material I plan to use with the Online Safety Lead.

### **Video conferencing**

I will only use the conferencing tools that have been identified and risk assessed by the school leadership, DPO (Data Protection) and DSL. A school-owned device should be used when running videoconferences, where possible.

### **User signature**

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as a governor.

Signature:

Date:

Full Name:

Job title

## **Appendix B - Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers**

### **Haileybury Turnford**

**Online safety lead: Maxine Goodes**

**Designated Safeguarding Lead (DSL): Maxine Goodes**

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on record, and you should retain your own copy for reference.

Internet, mobile and digital technologies are part of our daily working life, and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with the Online Safety Lead. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply, and police involvement will be sought.

The school's online safety policy will provide further detailed information as required.

### **Internet Access**

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL and an incident report completed.

### **Online conduct**

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the Online Safety Lead.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, principal and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to students and/or parents/carers.

Should I need to share my professional details, such as mobile phone number or email address, with parent/carers, this must be agreed in advance as an acceptable approach with the Online Safety Lead.

### **Social networking**

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or students on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or students. I understand the need to separate my professional role from my private friendships and I will not become 'friends' with ex-students who are also known to be 'vulnerable' young people up to the age of 25.

Information can be shared with students over 13 and parents/carers through an organisational social

network site/page e.g. on Facebook or Twitter, but never through a personal account or site. In my professional role in the school, I will never engage in 1-1 exchanges with students or parent/carers on personal social network sites.

My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or students. Privileged information known because of my work in the school must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

### **Passwords**

I must clarify what access I may have to the internet and/or school systems. If I have access of any kind, I understand that there is no occasion when a password should be shared with a student or anyone.

### **Data protection**

I will follow all requirements for data protection explained to me by the school. These include:

- I must consult with the school before making any recordings, photographs and videos. Once agreed, these must be made on a school device.
- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.

### **Images and videos**

I will only upload images or videos of staff, students or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of tuition or wider school activities on any personal device. School devices can be used for this purpose or, in the case of 1:1 tuition, student's or parent/carer devices can be used, with parent/carer agreement.

Internet, mobile and digital technologies provide helpful recording functions, but these cannot be made on a teacher's personal device. Recordings can be made with the child's and parent/carer's agreement on a school device, an organisational device approved by the principal/DSL, or a young person's or parent/carer's own device.

### **Use of Email**

I will only use my professional email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my professional email addresses for personal matters.

### **Use of personal devices**

I understand that when working in the school I should at no time put myself in a position where a safeguarding allegation can be made against me because of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the principal.

I will only use approved personal devices in designated areas and never in front of students. This therefore precludes use of specialist apps on personal devices. A school device could be used to access specialist apps that support student learning. Students can also be encouraged, but not required, to access such apps on their own devices if allowed by the school and with parent/carer agreement.

### **Additional hardware/software**

I will not install any hardware or software on school equipment without permission of the Online Safety

Lead.

### **Promoting online safety**

I understand that online safety is part of my responsibility, and I will always promote positive online safety messages, including when setting homework, rehearsal or skill practice or when providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any behaviour (of staff, governors, visitors, students, or parents/carers) which I believe may be inappropriate or concerning in any way to the DSL or the Online Safety Lead.

### **Classroom management of internet access**

I will pre-check for appropriateness all internet sites used in the classroom or during a tutoring session; this will include the acceptability of other material visible, however briefly, on the site. I will not free surf the internet in front of students.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the Online Safety Lead.

### **Video conferencing**

I will only use the conferencing tools that have been identified and risk assessed by the school leadership, DPO and DSL. A school-owned device should be used when running videoconferences, where possible

### **User Signature**

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation's contract with the school.

Signature ..... Date .....

Full Name ..... (Please use block capitals)

Job Title/Role .....

## **Appendix C - Requirements for visitors, volunteers and parent/carers helpers (Working directly with children or otherwise)**

**School name** Haileybury Turnford

**Online safety lead:** Maxine Goodes

**DSL:** Maxine Goodes

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

Please raise **any** safeguarding concerns arising from your visit immediately with the principal and/or DSL

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.
- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any exception must be pre-arranged.
- I will not give out my personal details such as mobile phone number, email address, and social media account details to students. Where appropriate I may share my professional contact details with parents/carers provided the DSL or principal is informed before I leave the school.
- I understand my visit to the school may give me access to privileged information about students, staff, school systems and plans. Such information should never be shared online, including on social media sites.
- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the principal.
- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free surf the internet in front of students. If I am in any doubt about the appropriateness of the content, I plan to use I will check with my contact in the school.



## Appendix D - Online Safety Acceptable Use Agreement: Students

- I will only use school IT equipment for school purposes.
- I will not download or install software on school IT equipment.
- I will only log on to the school network, other school systems and resources using my own school username and password.
- I will not reveal my passwords to anyone other than a parent/carer.
- I will not use my personal email address or other personal accounts on school IT equipment.
- I will make sure that all my electronic communications are responsible and sensible.
- I understand my behaviour in the virtual classroom should mirror that in the physical classroom.
- I understand that everything I search for, access, post or receive online can be traced now and in the future. My activity can be monitored and logged and if necessary shared with teachers, parents/carers and the police if necessary. I know it is essential that I build a good online reputation.
- I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to a member of staff if I am in school, or parent/carer if I am not in school.
- I will not give out my own or others' personal information, including name, phone number, home address, interests, schools or clubs or any personal image. I will report immediately any request for personal information, to a member of staff if I am in school or parent/carer if I am not in school.
- I should never post photographs, videos or livestream without the permission of all parties involved.
- I will not upload any images, videos, sounds or words that **could** upset, now or in the future, any member of the school community, as this is cyberbullying.
- I will be respectful to everyone online; I will treat everyone the way that I want to be treated. I will ensure that all my online activity, both in and outside school, will not cause distress to anyone in the school community or bring the school into disrepute.
- I will not respond to hurtful behaviour online but will report it. I have the right to block and will say no to any inappropriate or upsetting request.
- I will respect the privacy and ownership of others' work on-line and will always adhere to copyright.
- I will not attempt to bypass the internet filtering system in school.
- I will not assume that recent technologies can be brought into school and will check with staff before bringing in any device.
- I will not lie about my age to sign up for age-inappropriate games, apps or social networks.
- I understand that not everything I see or hear online is true, accurate or genuine. I also know that some people on the internet are not who they say they are and may have ulterior motives for assuming another identity that will put me at risk. I will gain permission from parents/carers before arranging to meet someone I only know on the internet.
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules, teachers will investigate, I may be disciplined, and my parents/carers may be contacted. If I break the law the police may be informed.

Dear Parent/Carer,

The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all students to be safe and responsible when using any IT. It is essential that students are aware of online risk, know how to stay safe and know where to go to report problems and access support.

Students are expected to read and discuss this agreement with you and then sign below to show they will follow the terms of the agreement. Any concerns or explanation can be discussed with the Online Safety Lead/Mrs Goodes.

Please can you also sign and return the parent/carers agreement below.

This document will be kept on record at the school.

### **Student agreement**

Student name.....

I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

Student signature.....

### **Parent(s)/Carer(s) agreement**

Parent(s)/Carer(s) name(s).....

I/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child. I/we agree to support them in following the terms of this agreement.

I/we also agree not to share school related information or images online or to post material that may bring the school or any individual within it into disrepute.

(Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, students and parents.)

I/we also agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren, unless there is a pre-specified agreement. I/we understand that when on school premises but not in a designated area where phones can be used, they must be switched off and out of sight.

Parent(s)/carer(s) signature(s) .....

Date .....

## **Appendix E - Online safety policy guide - Summary of key parent/carers responsibilities**

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- Parents/carers are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for students.
- Parents/carers may only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises that include anyone other than their own child, unless there is a pre-specified agreement with individuals and parents/carers. When a parent/carers is on school premises but not in a designated area, their phone/s must be switched off and out of sight.
- Parents/carers should not assume that students can bring technological devices to school and should always check the school policy.
- All cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.
- The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school's name or logo in any form.
- Any parent/carers distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, students and parents/carers.

Please see the full online safety policy in the policies section on the school website.

## **Appendix F - Guidance on the process for responding to cyberbullying incidents**

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community many cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Students should report to a member of staff (e.g. class teacher, principal) and staff members should seek support from their line manager or a senior member of staff.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecently images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the principal so that the circumstances can be recorded.
- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will investigate.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary, the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking are also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

## **Appendix G - Guidance for staff on preventing and responding to negative comments on social media**

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information. The online safety policy, see especially Appendix F (Online safety policy guide - Summary of key parent/carer responsibilities), clarifies that no other social media platforms should be set up using the school's name or logo.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

- Collect the facts

As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.

If the allegations against a member of staff or a student are of a serious nature, these will need to be formally investigated. This may involve the police and the principal will need to follow the school's safeguarding procedures.

If there is a risk of considerable damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.

Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

- Addressing negative comments and complaints

Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available.

The meeting must:

- Draw attention to the seriousness and impact of the actions/postings;
- Ask for the offending remarks to be removed;
- Explore the complainant's grievance;
- Agree next steps;
- Clarify the correct complaints procedures.

If the meeting does not resolve the issue, the parents must be informed that the school will need to take the matter further. This may include:

- Reporting the matter to the social network site if it breaches their rules or breaks the law;
- Reporting the matter to the police if it breaks the law, e.g. if the comments are

threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking are also a crime.

If inappropriate postings continue or the original material is not removed, a second meeting is advisable to re-iterate the seriousness of the matter.

## **Appendix H –links to relevant GDPR policies**

[GDPR Data Breach Guidelines 27-09-2021.pdf](#)

[GDPR Data Protection Policy 27-09-2021.pdf](#)

[GDPR Data Retention Policy 27-09-2021.pdf](#)

[GDPR Data Security Policy 27-09-2021.pdf](#)

[GDPR Privacy Notice Gvnrs Trustees 27-09-2021.pdf](#)

[GDPR Privacy Notice Parents Carers 27-09-2021.pdf](#)

[GDPR Privacy Notice Staff 27-09-2021.pdf](#)

[GDPR Records Retention Schedule 27-09-2021.pdf](#)

[GDPR SAR Policy 20-03-2023.pdf](#)