Westbrook Hay Prep School

7h E-SAFETY POLICY

Our mission is to develop happy, confident and successful children who are well prepared for their future.

INTRODUCTION

It is the duty of Westbrook Hay Prep 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, 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.

This policy should be read in conjunction with the Child Protection and Safeguarding Policy, ICT Acceptable Use Policy, Bring Your Own Device Policy, Taking, Using and Storing Images of Children Policy, Social Media Policy and GDPR Privacy Policies.

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 Westbrook Hay Prep School, we understand the responsibility to educate our pupils on e-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 e-safety and listening to their fears and anxieties as well as their thoughts and ideas.

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. 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.).

ROLES AND RESPONSIBILITIES

The Governing Body

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

Head Teacher, Designated Safeguarding Lead (DSL) and the Executive Group

The Head Teacher is responsible for the safety of the members of the school community and this includes responsibility for e-safety. The Head Teacher has delegated day-to-day technical and teaching responsibility to the Head of IT while the DSL maintains a safeguarding overview.

In particular, the role of the Head Teacher, DSL and the Executive Group is to ensure that:

- staff, in particular the Head of IT are adequately trained about e-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 e-safety in connection to the school.

Head of IT

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

IT staff

The school's technical staff have 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 assisting in 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 report inappropriate usage to the Head of IT.

Teaching and support staff

All staff are required to read the Acceptable Use Policy and sign a statement during induction, before accessing the school's systems. As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

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.

Parents and carers
Westbrook Hay Prep School believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-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 Acceptable Use Policy.

EDUCATION AND TRAINING

Staff: awareness and training
New staff receive information on Westbrook Hay Prep School's e-Safety and Acceptable Use policies as part of their induction.

All staff with computer access receive regular information and training on e-safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety. All supply staff and contractors receive information about e-Safety as part of their safeguarding briefing on arrival at school.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. These behaviours are summarised in the Acceptable Use Policy. 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 e-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 My Concern entry must be completed by staff as soon as possible if any safeguarding incident relating to e-safety occurs.

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

The school provides opportunities to teach about e-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 PSHE (SCARF), by presentations in assemblies, as well as informally when opportunities arise.

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 Safeguarding Team and/or the Head of IT as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

Parents

The school seeks to work closely with parents and guardians in promoting a culture of e-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 child when they use electronic equipment at home. The school therefore arranges discussion evenings for parents when an outside specialist advises about e-safety and the practical steps that parents can take to minimise the potential dangers to their child without curbing their natural enthusiasm and curiosity.

POLICY STATEMENTS

USE OF SCHOOL AND PERSONAL DEVICES

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for school work. When they are not using a device staff should ensure that it is locked to prevent unauthorised access. Devices issued to staff are encrypted, to protect data stored on them.

Staff are referred to the BYOD Policy in the Staff Handbook for further guidance on the use of non-school owned electronic devices for work purposes.

Staff at Westbrook Hay Prep School are permitted to bring in personal devices for their own use. Staff may use such devices in school staffrooms or during non-contact break times when no children are present, or when emergency circumstances dictate (e.g. to call for medical assistance when on the sports field).

In line with EYFS (includes Reception) regulations, personal mobile devices are not allowed in any EYFS setting, where this setting is defined as any area where EYFS pupils are present or are reasonably expected to be present. This is the case for visitors and staff. The use of mobile phones is permitted in the Pre-Prep staff room and the Pre-Prep School Office. Parents may take photographs of their own child, using their mobile phone, at public performances but should not post these photographs on social media is any children is visible in the photo.

Personal telephone numbers, email addresses, or other contact details may not be shared with pupils or parents/carers and staff may not contact a pupil or parent/carer using a personal telephone number, email address, social media, or other messaging system.

Staff who are teaching outdoors (i.e. sports staff), or who are on a school trip are permitted to receive calls from the school on their personal device. Staff should explain to the children who

is calling them and why they need to receive the call. The call should be ended as soon as possible and the phone placed back out of site.

Pupils

If pupils bring in mobile devices, once express permission from the Head Teacher has been received (e.g. for use during the journey to and from school), they should be kept switched off handed in to the school office at the start of the day and collected as they leave school. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the school SENCO will make appropriate arrangements.

USE OF INTERNET AND EMAIL

Staff

Staff must not access social networking sites, personal email, any website or personal email which is unconnected with school work or business from school devices or whilst teaching / in front of pupils. Such access may only be made from staff members' own devices whilst in staff-only areas of school. The exception is those members of staff who may be adding information to the school's owned and controlled social media sites.

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 Head of IT 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 IT.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring Westbrook Hay Prep 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:
- making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
- using social media to bully another individual; or
- posting links to or endorsing material which is discriminatory or offensive.

Under no circumstances should school pupils or current parents be added as social network 'friends' or contacted through social media.

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Staff should refer to the Westbrook Charter for further advice. Under no circumstances may staff contact a pupil or parent / carer using any personal email address. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

Pupils

All pupils are issued with their own personal school email addresses for use on our network and offsite. 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. Pupils should be aware that email communications through the school network and school email addresses can be 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 purposes, pupils should contact the Head of IT 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 IT or another member of staff.

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 any member of staff they feel comfortable talking to. Deliberate access to any inappropriate materials by a pupil will lead to the incident being dealt with under the school's Behaviour Management Policy. Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work pupils should contact the Head of IT for assistance.

DATA STORAGE AND PROCESSING

The school takes its compliance with the Data Protection Act 1998 (updated December 2020) seriously. Please refer to the Data Encryption Policy and the Acceptable Use Policy for further details.

Staff and pupils are expected to save all data relating to their work to their Chromebook or PC or to the school's central server / Google Drive Account.

Staff devices should be encrypted if any data or passwords are stored on them. The school has banned all portable media for the transference of data.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. Any personal data should be stored in the School owned and managed Google Drive.

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 IT and the School's Privacy Officer.

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.

Pupils and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers except KS1 and Lower KS2 pupils who will use a simpler format, which should be changed every term for staff and annually for pupils;
- only write passwords down in their school planner (and only to sites that contain no personal information); and
- not share passwords with other pupils or staff.

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. in line with the Taking, Storing and Using Pictures of Children Policy

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy and the Acceptable Use Policy, Taking, using and Storing Images of Children and EYFS Policies 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 share, publish or distribute images of others. Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website (see Parent Contract / Acceptable Use Policy for more information).

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. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

MISUSE

Westbrook Hay Prep 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 Local Authority Designated Office (LADO). 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 LADO.

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with [the school's policies and procedures (in particular the Child Protection and Safeguarding Policy).

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

COMPLAINTS

As with all issues of safety at Westbrook Hay, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it.

Complaints should be addressed to the Head of IT in the first instance, who will liaise with the leadership team and undertake an investigation where appropriate. Please see the Complaints Policy for further information.

SAFEGUARDING CONCERNS

Incidents of or concerns around safeguarding and e-safety will be recorded using My Concern and reported to the Designated Safeguarding Lead (DSL), or, in their absence, a Deputy DSL in accordance with the school's Child Protection and Safeguarding Policy.

Reviewed by Andy Lloyd, Assistant Head (Operations), Head of IT 02.10.21
Approved by Matthew O'Donnell, Governor and Chair of the IT and GDPR Committee 07.10.21

This policy with be reviewed annually or on line with any changes to stature or regulation