Digital Use Policy

Whole school	WEBSITE
Statutory? No	
Reviewed February 2018	
Next review February 2019	

INTRODUCTION

New technologies have become integral to today's society, so that digital use is now a facet of life within school and beyond for students and staff. Furthermore, advances in digital technology over recent years have changed not only the way in which we engage with each other and with the world but also the ways in which we learn.

This policy aims to outline the scope and the management of digital use at King's Ely and applies to all members of the school community (including staff, students, volunteers, parents and guardians) who have access to and are users of digital technologies, both in and out of school.

DIGITAL SAFETY

New technologies can put young people and staff at risk, both within and outside of school. '*Digital Safety*' highlights the need to educate users about the benefits and risks of using technology; providing safeguards and awareness to enable students and staff to control their online experiences.

King's Ely recognises its duty of care to safeguard and promote the welfare of its students and the duty to take all reasonable measures to protect the health and safety (including digital safety) of its students and staff. The school has an obligation under the Prevent Duty[1] to have in place a robust IT filtering and monitoring procedure, aimed to prevent the online radicalisation of pupils. To this end, the school uses iBOSS and Firesphere for filtering and monitoring web browsing of users using the school's infrastructure and Libra ESVA for filtering and putting into "quarantine" suspicious/malicious/content specific email. This allows the School's system to control access to certain websites/services at certain times by age group/staff and to automatically bring to the attention of appropriate managers (including the school's named Prevent lead) any use of the school network to access certain websites or to search for terms linked with terrorism, radicalisation or the undermining of fundamental British values.

PROMOTING DIGITAL SAFETY

King's Ely seeks to embrace all the benefits that modern technology provides for the education of its students. However, the potential for misuse and abuse of digital technology is significant and King's has a duty of care to ensure that students are able to use ICT, including the internet and related communication technologies, appropriately and safely. New technologies can put young people at risk, both within and outside of the school. The school aims to provide the necessary safeguards to King's Ely Safeguarding Policy 9 help ensure that those responsible have done

[1] a duty under S.26 of the Counter-Terrorism and Security Act 2015 "*to have due regard to the need to prevent people from being drawn into terrorism*".

everything that could reasonably be expected of them to manage and reduce these risks. All staff at King's Ely receive ESafety Training and are regularly updated on any developments in the field of digital safety as required or via the termly safeguarding bulletins. Furthermore, the DSOs have undertaken the NSPCC 'Keeping Children Safe Online V2' online course or CEOP Ambassador Training. This level of training is being rolled out to all PSHE leads and ICT coordinators across all sections of the school. Specialist speakers are also invited to provide various INSET sessions for staff about on-line/Cyber risks in relation to protecting children and themselves.

Parents are often invited to attend briefings from various ESafety/Cyber protection visiting speakers as well as being informed periodically about on-line/cyber related trends and warning via newsletters.

The Principal is responsible for ensuring the safety of members of the school community (this includes ensuring that pupils' exposure to potential risks while using the internet is limited by having in place age appropriate filtering and monitoring systems), although the day-to-day responsibility for digital safety is delegated to the Digital Safety Coordinator, the Designated Safeguarding Lead and the Head/Vice Principals of the relevant section of the school.

Digital Safety Coordinators[2]:

- take day to day responsibility for digital safety issues and have a leading role in establishing and reviewing the relevant policy documents;
- provide training opportunities and advice for staff (paid and unpaid), parents and pupils where necessary;
- receive reports of digital safety incidents and create a log of incidents to inform future digital safety developments;
- report to the school's Leadership Team and the Prevent or Designated Safeguarding Lead.

The Business Manager is responsible for ensuring that:

- the school's ICT infrastructure is secure and is not open to misuse or malicious attack;
- users may only access the school's networks through a regime of properly enforced password protection;
- the use of the network (including remote access and email) is regularly monitored in order that any misuse or attempted misuse can be reported immediately for further investigation as appropriate;

[2] In KES and KEI the role of Digital Safety Coordinator is fulfilled by the Vice Principal Pastoral and in KEJ the role is undertaken by the Head and Assistant Head KEJ

- the use of the school network to access websites or to search for terms linked with terrorism, radicalisation or the undermining of fundamental British values are reported to the school's named Prevent lead.

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of digital safety matters and of the current school procedures[3]
- they monitor digital activity in lessons and in any extra-curricular school activities and they report any suspected misuse or problem to the Digital Safety Coordinators for further investigation;
- digital communications with students take place within clear professional boundaries. Staff should not share any personal information with a student and they should not request any such information from a student, other than that which might be appropriate as part of their professional role. To this end, staff should ensure that all communications are transparent and open to scrutiny and should keep in mind the following points:
    - staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of such images and these may only be stored on the school systems. For EYFS, these images should only be taken on school equipment; the personal equipment of staff - must not be used for such purposes (see below);
    - care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individual or the school into disrepute;
    - pupils must not take, use, share, publish or distribute images of others without their permission;
    - photographs published on the school website that include students should be selected carefully and comply with good practice guidance on the use of such images.

Pupils should ensure that they:

- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good digital safety practice when using digital technologies out of school and realise that the school's behaviour policy also covers their actions out of school;
- adhere to the specific guidelines set out in the *Bring Your Own Device Procedure* and the *Acceptable Use Procedure(s)*

[3] Bring Your Own Device (BYOD) Procedure; Acceptable Use Procedure

All staff, pupils and parents are responsible for reporting any suspicion, threat or concern about use of digital/on-line platforms in a manner that may cause harm to any child, member of staff or the wider-community. Any such concerns must be reported through the School's normal reporting arrangements (as detailed on page 17 of the Safeguarding Policy).

DIGITAL LEARNING

Within education, the advances in digital technology offer great opportunities for students and teachers. The traditional model of the teacher imparting knowledge to the passive leaner is turned on its head. Today's pupils understand the world of technology and are confident enough to search out knowledge and bring it back to the classroom.

Whilst regulation and technical solution are very important, their use must be balanced by educating pupils to take a responsible approach. Digital Safety education will be provided in the following ways:

- a planned digital safety programme provided as part of ICT/ PSHE/ other lessons throughout the school, as appropriate for the age of the pupil, with the aim of reinforcing key digital safety messages (ensuring pupils understand the risks posed by others who use the internet and social media to bully, groom, abuse or radicalise[4] young people) as part of a planned programme of tutorial/pastoral activities;
- when using digital images, staff are to inform and educate students 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 and via apps.

As part of digital learning at King's Ely, the school has:

- Developed IT infrastructure to store and distribute information, including assignments and digital media;
- Made information available to pupils in the form of online resources and applications;
- Prepared for the behavioral changes needed to ensure that new types of technologies are used responsibly, productively and cohesively;
- Supported and developed teaching staff to ensure they are engaged in new teaching and learning practice;
- Introduced BYOD for all pupils in years 7 to 13.

King's Ely's approach to the management of access to 3G and 4G on the school site is through a programme of education and robust supervision.

[4] The use of social media for online radicalisation (July 2015)

DIGITAL (SOCIAL) MEDIA

Social media describes the sharing and dissemination of various forms of media through online social interactions and encompasses many variations of online media. Examples include blogs, micro-blogs (Twitter), podcasts, wikis (such as Wikipedia), message boards, social book marking websites (Reddit), social networking sites (Facebook, MySpace) and media content sharing websites (such as Pinterest, YouTube).

It is necessary, when engaging in social media activity, that King's Ely staff and pupils act responsibly, safely and in a way that reflects the values and reputation of the organisation. King's Ely Digital (Social) Media procedures are in place to provide guidance and regulation in this area (please see Appendix). It should be noted that any deliberate action designed to bring the school's name into disrepute may result in suspension or permanent exclusion (please see the King's Ely Behaviour Policy – as per DfE guidance, Behaviour and Discipline in Schools (2016), teachers may discipline pupils for non-criminal bad behavior off site).

For a detailed list of any sanctions relating to contravening Digital Use, Cyber Bullying or Safeguarding policies, please refer to the School's behaviour Policy and the Staff Code of Conduct.

PERSONAL DATA

Personal data is managed in accordance with statutory requirements. Further details about how personal data is managed, stored and processed can be found in the School's Data Protection Policy and the School's Privacy Statement.

USE OF THE SCHOOL'S IT INFRASTRUCTURE BY VISITORS

Visitors are able to use upon request a King's Ely Guest Wi-Fi password. Users are warned prior to being given the password that it must not be passed onto anyone, especially King's Ely school children, that whilst using the School's infrastructure, their web browsing activity will be monitored and logged by our systems and that whilst using the service, they must not use it for any inappropriate activity.

The password of the Guest Wi-Fi is changed on a regular basis and only issued to a limited number of staff to provide to visitors.

APPENDIX ONE: DIGITAL USE – POLICIES AND PROCEDURES

Digital Use is embedded in all areas of school life. It forms part of key school policies and is supported by the following documents.

POLICIES				
Digital Use Policy Outlines the concept of digital use at King's Ely.	**Behaviour Policy** At King's Ely the sanctions for digital misuse are clearly set out in the whole school Behaviour Policy.	**Safeguarding Policies** ➢ **Safeguarding (including Child Protection) Policy** – sets out the school's commitments to digital safety; ➢ **Social Respect (Anti-Bullying) Policy & Strategy** – contains the school's response to Cyberbullying.	**Curriculum Policy** At King's Ely the curriculum incorporates scientific and technological (including the use of ICT) learning and experience;	**Data Protection Policy** Provides for the management of personal data in line with statutory requirements.
PROCEDURES				
➢ Acceptable Use Procedures (KES/KEI; KEJ; Staff) ➢ BYOD Procedure ➢ Social Media Procedure (staff) ➢ Social Media Guidelines ➢ Twitter Procedure			➢ Teaching & Learning Procedure	➢ Data Protection procedures (work in progress); ➢ Data Protection Audit (in process preparing for GDPR)
OTHER				
	➢ Employment Manual ➢ Pupil Handbook ➢ Staff Code of Conduct	➢ ESafety Guidance for Students / for Parents & Guardians ➢ INSET – safeguarding and online safety ➢ Terms & Conditions (*Photographs or Images*)	➢ Digital Safety as part of PSHE/PD	

APPENDIX TWO: MONITORING OF AND RESPONSE TO INAPPROPRIATE WEB SEARCHES AND PERSONAL USE OF THE SCHOOL'S MONITORED IT INFRASTRUCTURE AND HARDWARE *(Please read in conjunction with the school's Staff Code of Conduct, Child Protection, Social Respect and IT Acceptable Use policies)*

Safeguarding duty	Mitigation of risk to KE community	Responsibility	Review procedure and timescale
The monitoring of email traffic via the school IT systems and school email addresses *(NB - Mobile devices using other networks, are not filtered by the school)* (Terminology and the details of the filters applied are contained in Appendix 3)	The use of specific vocabulary in an email or the attaching of a dubious item to an email, will mean that the emails is filtered to the Designated Safeguarding Officers (DSOs) including the Designated Safeguarding Lead (DSL/Prevent lead)	IT technicians for the maintenance of the auto filtering to DSOs - for day to day implementation of the filters and conveying information to DSOs Designated Safeguarding Officers (DSO) in each section responsible for intervention when concerns are sent to filtering@kingsely.org Designated Safeguarding Lead (DSL/Prevent lead) in the case of possible radicalisation under the "Prevent" duty	Minute by minute checking of all email traffic via filtering@kingsely.org email address As potentially concerning messages are reported by the system, they are passed immediately to the DSO in the student's section of the school by the system. Effectiveness considered by KE SLT at regular intervals each term and formally reported as part of the annual Child Protection Review for Cambridgeshire County Council and the School's Board of Governors
The monitoring of web searches made via the school's internet connections to access websites or to search for terms linked with, safeguarding, crime, terrorism, radicalisation or the undermining of fundamental British values. (Terminology and the details of the filters applied are contained in Appendix 3)	iBOSS software is used to monitor all searches conducted by staff and students at King's Ely via the School's wifi and wired networks. Bespoke list of terms and words which could be linked to abusive behaviour, grooming, crimes and radicalisation are used as the trigger for any searches to be blocked and referred to the DSOs. Full reports are generated once a week and are also automatically sent to DSOs each day in each section of the school.	IT technicians for the day to day operation of the filter and the automatically generated daily/weekly email reports to DSOs DSOs for the response to any searches or patterns of searches giving rise to potential safeguarding concerns DSL* for the response to any searches or patterns of searches giving rise to any concerns under the "Prevent" duty *(*Any DSO in the absence of the DSL)*	Weekly via the formal reporting to the sections and Prevent Lead but the filters are active at all times. Daily check by DSOs on searches and as they happen alerts for HIGH RISK searches. The review of searches containing trigger words inform the school's response and any referrals or intervention by school and/or partner agencies. Effectiveness considered by KE SLT regular intervals each term and formally reported as part of the annual Child Protection Review for Cambridgeshire County Council and the School's Board of Governors

APPENDIX 3 – FILTERING BY CATEGORIES AND ACTIVITY

Action on the school system or wi-fi	Measure in place
Internet searches	Filtered using iBoss and Firesphere (anti-malware download protection) software and key word lists applied by the Network Manager
Email content	Filtered using Libra ESVA
Virus Protection	Libra ESVA scans all incoming and outgoing emails for virus content. Client machines (PCs) and Servers are protected by Sophos Cloud X anti-virus

iBoss filtering software flags "high risk" internet searches on an immediate, daily and weekly basis to a DSO in each section of King's Ely

Each "high risk" entry contains:

Date, time, name of searcher, secure IP number, the URL address, the nature of the search terms entered by the user and whether the search was blocked or permitted.

iBoss filtering software highlights blocked internet searches on an immediate or weekly basis to a DSO in each section of King's Ely

Each "blocked" entry contains:

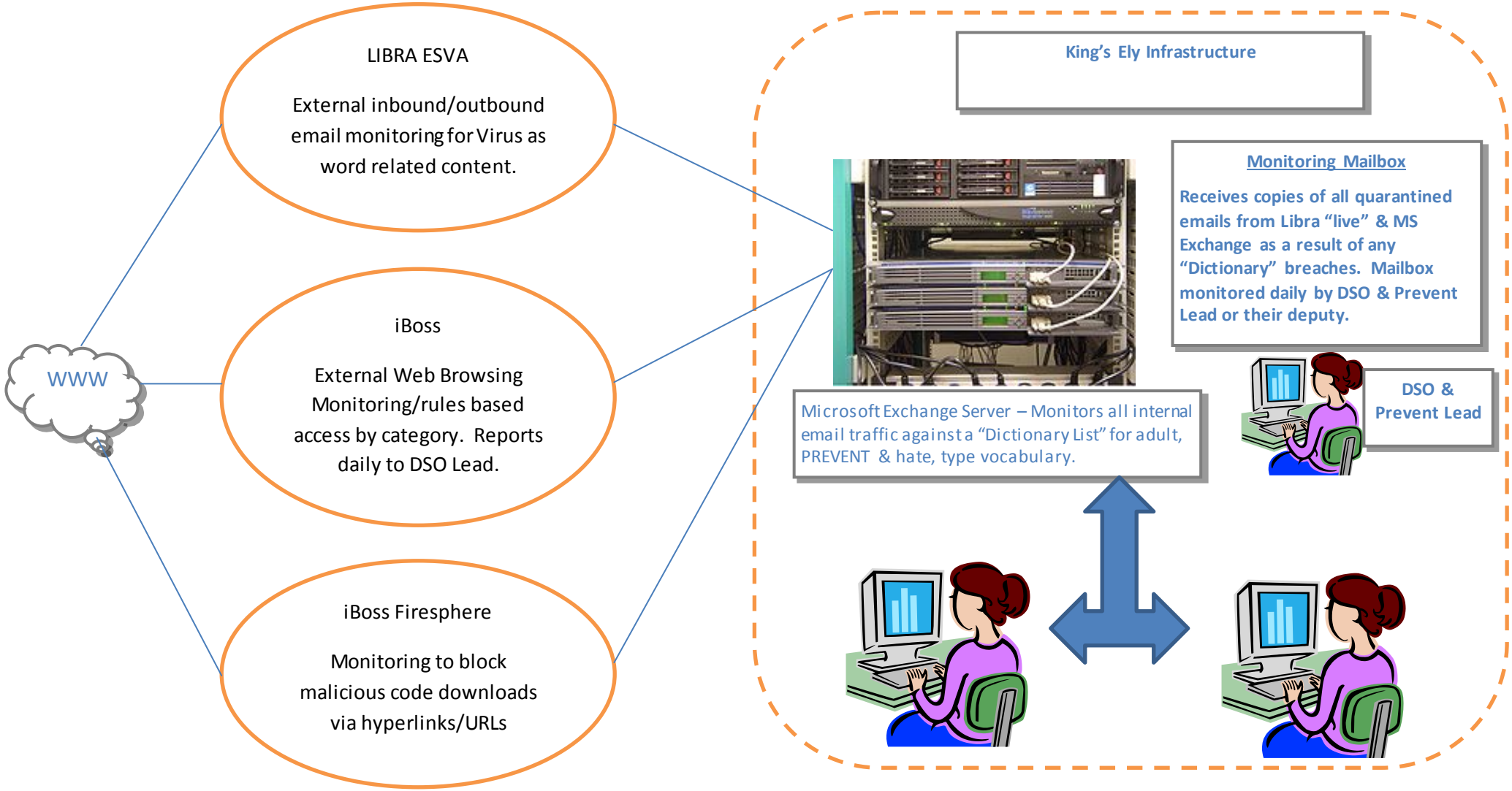
Date, user, URL/Event, secure IP number, category, blocked or allowed

iBoss has an imported and relatively static list of dictionary search words but is updated constantly from shared global intelligence about inappropriate and "dangerous" URLs/websites.

Libra ESVA software filters and highlights all external incoming and outbound (from the school's infrastructure) emails with blocked content. Libra's reference vocabulary lists are updates constantly from lists produced by the Home Office. Internal emails are scanned for inappropriate words using MS Exchange.

A diagram overleaf shows how the systems interact/where they sit between the Internet (external to King's Ely infrastructure) and the internal systesm

King's Ely – Email and Web Monitoring systems (Anti-Virus, Safeguarding & Prevent responsibilities)



APPENDIX 4 - EMAIL ACCOUNT PROTOCOL FOR STAFF AND STUDENTS LEAVING KING'S ELY

All staff and pupils are provided with a school email address when they need one for school purposes.

Upon leaving King's Ely, the following will apply:

- Upon resignation, retirement or end of contract, staff will be able to access their email account for a period of one month following their departure (for academic staff leaving at the end of the summer term, this is in effect one month after 31 August).
- Former students will be able to access their email accounts up until the start of the next term.
- Staff and students will be removed from email distribution lists upon departure from school (for students and academic staff, this will mean 31 August if leaving at the end of the summer term).
- Staff who are dismissed or who resign whilst under any form of investigation or disciplinary procedures will lose access immediately to their email account and/or any remote systems access. The same will apply to any pupils expelled or withdrawn for behavioural reasons, as deemed appropriate by the Principal/Head of Section[5].
- Any staff with system administration rights will lose these system permissions immediately upon departing King's Ely, whilst maintaining normal user email access as for other former staff.
- Staff and pupils should ensure all email accounts and storage drives are void of personal material by the time their account is disabled (school email accounts should not be used routinely for personal use). The full content of email accounts/Z Drives may be deleted or transferred to a successor (in the case of staff).
- Departing Governors will have remote access revoked from the final day of their tenure. School Email access will continue for a month after their departure.
- Unless stated otherwise, remote access to school systems will cease in the same timeframe as email access.
- For the sake of clarity, this does not apply to those absent on long-term sick or whilst absent on Maternity, Paternity or Shared Parental Leave (in all cases, email/account permissions for remote access remain).

Staff on Zero hours contracts (internal "supply" staff):

- Where staff need to have access to school email whilst engaged on zero hours contracts they will have their email account enabled just prior to/upon starting each engagement and

[5] In certain circumstances, the staff member or pupil will be allowed access to their school account to forward any personal or investigation/disciplinary related material to their personal email address. If necessary, pupil's school work will need to be sent a personal email address.

disabled at the end of each period of work[6]. Such staff will not routinely have remote access to any school IT systems or be on general school email distribution lists whilst they are not actively engaged/working for King's Ely.

Transitional arrangements:

- Any past staff and students, including those on zero hours contracts will have their names removed from all distribution lists with immediate effect.
- Any staff or pupils who have left King's Ely will be provided with one month's notice that their email account and will be disabled before being deleted permanently. For some staff, the content of a mailbox/Z Drive may be transferred to a suitable colleague.
- Access to the Remote Desktop Server, Horizon View Desktop Services, Securelink, Firefly and any other systems/school associated accounts will be denied at the end of the one month's notice period.

[6] Where zero hours staff are engaged by King's Ely frequently within any period, with the agreement of the Head of section, their email account can remain active.