Bosworth Independent College

Online Safety Policy

Reviewed	July 2020
Next Review Date	July 2021
Lead for Review	DSL

Contents

Scope of the Policy

This policy applies to all members of the College (including staff, volunteers, students, parents/carers, visitors) who have access to and are users of College digital technology systems, both in and out of the College.

The Education and Inspections Act 2006 empowers Heads/Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the College site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the College, but is linked to membership of the College. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Bosworth College Behaviour Policy.

The College will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that take place out of College.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the College:

Principal and Senior Leaders

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the College community. Day to day responsibility for online safety is delegated to the Online Safety Officer (OSO). This is combined with the role of Designated Safeguarding Lead (DSL).
- The Principal is aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (See below.). In the event that the Principal is not available the Chair of Governors must be contacted.
- The Principal is responsible for ensuring that the OSO and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal will ensure that there is a system in place to allow for monitoring and support of those in the College who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the OSO.

OSO (Online Safety Officer)

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the College's online safety policies/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff.

- Liaises with the Local Authority or other relevant bodies.
- Liaises with College technical staff.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Reports regularly to Senior Leadership Team.

The OSO is trained in Online Safety issues and is aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Online-bullying

In Meetings with the Principal, the Senior Leadership Team, the Head of ICT, Magma and other relevant parties the OSO ensures that issues regarding online safety and monitoring the Online Safety Policy include the impact of initiatives. Items may include (but are not limited to):

- The production/review/monitoring of the College Online Safety Policy/documents.
- The production/review/monitoring of the College filtering policy and requests for filtering changes.
- Mapping and reviewing the online safety/digital literacy curricular provision, ensuring relevance, breadth and progression.
- Monitoring network/internet/incident logs.
- Consulting stakeholders, including parents/carers and the students, about the online safety provision.

Network Manager/Technical staff

The Network Management is carried out by the Magma Group. They are responsible for ensuring:

- That the College's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the College meets required online safety technical requirements and any other guidance or good practice that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- That the filtering policy and software is applied and updated on a regular basis and that its implementation is not the sole responsibility of any one person.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network, internet, VLE and remote access email is regularly monitored in order that any misuse can be reported to the Principal/OSO for investigation and, if appropriate, action and/or sanction.
- That monitoring software/systems are implemented and updated as compliant with College policies such as the Safeguarding Policy and according to best practice.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current College Online Safety Policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy (AUP) which is renewed annually
- They report any suspected misuse or problem to the Principal/OSO for investigation, action or sanction
- All digital communications with students/parents/carers should be on a professional level and only carried out using official College systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Students understand and follow the Online Safety Policy and Acceptable Use Policies
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other College activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned, students are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Students

- Are responsible for using the College digital technology systems in accordance with the Student Acceptable Use Agreement.
- Should develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of College and realise that the College's Online Safety Policy covers their actions out of College, if related to their membership of the College.

Boarding Staff and Parents/Carers

Boarding staff and Parents/Carers play a crucial role in ensuring that their students and children understand the need to use the internet/mobile devices in an appropriate way. The College will take every opportunity to help parents understand these issues through emails, letters, the College website/information about national/local online safety campaigns. Parents and carers will be encouraged to support the College in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at College events.
- Access to parents' sections of the website/VLE and on-line student records.

- Their children's personal devices in the College (where this is allowed)

Visitors

Visitors (e.g. visiting speakers or attendees of conferences and CPD events) who access College systems as part of the wider College provision will be expected to follow College rules. Guest Wi-Fi is provided with no access to internal administrative, student or staff areas of the College network.

Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety/digital literacy is therefore an essential part of the College's online safety provision. Students need the help and support of the College to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided as part of Computing, PHSE and other lessons and are regularly revisited.
- Key online safety messages are reinforced in lessons, activities and during boarding time such as Evening Study Hall or informally in Boarding Houses.
- Students are taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students are helped to understand the need for the student Acceptable Use Policy agreement and encouraged to adopt safe and responsible use both within and outside College.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that students are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or

other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so must be on writing so it is auditable and must include clear reasons for the need.

Education – Parents/Carers

The College acknowledges that some parents and carers may have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. Any advice and support for parents aims to be respectful but effective.

Education & Training – Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced through Educare. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety instruction as part of their induction programme, ensuring that they fully understand the College Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the appraisal process.
- The OSO (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- The OSO (or other nominated person) will provide advice/guidance/training to individuals as required.

Training – Governors

Governors will take part in online safety training/awareness sessions, with particular importance for those who are members of any subcommittee or group involved in technology/online safety/health and safety /safeguarding. This may be offered through attendance at training provided by the Local Authority/ISI/ISA or other relevant organisation, or participation in College training if appropriate.

Technical – Infrastructure/Equipment, Filtering and Monitoring

The College will be responsible for ensuring that the College infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities: College technical systems will be managed in ways that ensure that the College meets recommended technical

requirements There will be regular reviews and audits of the safety and security of College's technical systems.

- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to College technical systems and devices.
- All users will be provided with a username and secure password by the College who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password if necessary. At Bosworth, students do not hold accounts on College servers. IT support and access is via students' Bosworth (Outlook) email account, Firefly account and through access to the internet via the College's filtered and monitored student Wi-Fi.
- The "master/administrator" passwords for the College ICT systems, used by the Network Manager (or other person) must also be available to the Principal or other nominated senior leader and kept in a secure place (e.g. College safe).
- The Magma Group is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (such as child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored.
- There is a clear process in place to deal with requests for filtering changes, including checks by Magma with relevant members of the SLT or the OSO.
- Internet filtering/monitoring should ensure that students are safe from terrorist and extremist material when accessing the internet. The College has provided enhanced or differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students, etc.).
- College technical staff regularly monitor and record the activity of users on the College technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed). In Bosworth's Anti-Cyber-Bullying Policy, students are encouraged to report their concerns to any staff and especially the DSL/OSO. This is summarised in the Student Planner.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the College systems and data. These are tested regularly. The College infrastructure and individual workstations are protected by up to date virus software.
- An agreed procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the College systems.
- Rules are included in the Staff AUP regarding the extent of personal use that users (staff/students/community users) and their family members are allowed on College devices that may be used out of College.
- An agreed policy and suitable privileges are in place that control staff downloading executable files and installing programmes on College devices.

- If staff use removable media (e.g. memory sticks/CDs/DVDs) on College devices they must ensure that personal data is only placed on the device if that is a necessity and that any date is protected either by password protecting individual files, or the entire media item.
- The College takes care to follow all safeguarding good practice (including as specified in the most recent 'Working Together to Protect Children' and 'Keeping Children Safe in Education') and to follow the Data Protection Act.

Mobile Technologies, Including BYOD

Mobile technology devices may be College owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the College's wireless network. The device then has access to the wider internet which may include the College's learning platform and other cloud-based services such as email or Firefly.

All users should understand that the primary purpose of the use of mobile or personal devices in a College context is educational. The use of mobile technology must be consistent with and inter-related to other relevant College polices including but not limited to the Safeguarding Policy, Behaviour Policy, Anti-Bullying and Anti-Cyberbullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the College's Online Safety education programme.

The College Acceptable Use Agreements for staff and students will give consideration to the use of mobile technologies.

Use of Digital and Video Images

The development of digital imaging technologies has created significant risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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. It is common for employers to carry out internet searches for information about potential and existing employees. The College will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

When using digital images, staff should 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.

Written permission from parents or carers will be obtained before photographs of students are published on the College website/social media/local press. Given the age of the College's students, students' permission also is obtained. This is included in the College's 'terms and conditions'.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at College events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly

available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images.

Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow College policies concerning the sharing, distribution and publication of those images. Those images should only be taken on College equipment, the personal equipment of staff should not be used for such purposes. See the Staff Code of Conduct.

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

Students must not take, use, share, publish or distribute images of others without their permission.

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

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

Students' work can only be published with the permission of the student and parents or carers.

Data Protection

Bosworth College fulfils its responsibilities under the General Data Protection Regulations. See the College's Data Protection and Freedom of Information Policy (GDPR).

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the College currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff & other adults				Students			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the College	***					***		
Use of mobile phones in lessons			***			***		
Use of mobile phones in social time	***				***			

Taking photos on mobile phones if subject agrees				***		***		
Use of other mobile devices e.g. tablets, gaming devices	***					***		
Use of personal email addresses in College , or on College network				***		***		
Use of College email for personal emails				***	***			
Use of messaging apps	***					***		
Use of social media			***			***		
Use of blogs			***			***		

- The official College email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the College policy - 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.
- Any digital communication between staff and students or parents / carers (email, social media, chat, blogs, FireFly, etc.) must be professional in tone and content. But staff are expected not to use social media for contact with parents. The College accepts no responsibility for adverse professional or disciplinary consequences.
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the College website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

Under Bosworth's Staff Code of Conduct, staff are

- Warned against the risks of contact with parents or communities outside College. Or of entries made on social media becoming public.
- Expected to ensure privileges and access to sites on which information or comment about the College appears never infringe good practice, professional standards or the GDPR.
- Not protected by Bosworth from adverse consequences for which they themselves are responsible. This is different to support and follow-up offered to staff who are the victims of inappropriate conduct by other staff or students.

Dealing with unsuitable/inappropriate activities

Some internet activity, e.g. accessing child abuse images or distributing racist material, is illegal and would obviously be banned from College and all other technical systems. Other

activities, e.g. cyber-bullying, would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a College context, either because of the age of the users or the nature of those activities.

The College believes that the activities referred to in the following section would be inappropriate in a College context and that users, as defined below, should not engage in these activities in/or outside the College when using College equipment or systems. The College policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination					X
	threatening behaviour, including promotion of physical violence or mental harm					X
	Promotion of extremism or terrorism					X
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the College or brings the College into disrepute				X	
Using College systems to run a private business					X	

Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the College				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)			X		
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce		X			
File sharing		X			
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. Youtube			X		

Illegal or Other Incidents

It is hoped that all members of the College community will be responsible users of digital technologies, who understand and follow College policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
  - incidents of ‘grooming’ behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - promotion of terrorism or extremism
  - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the College and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

College Actions & Sanctions

This Policy confirms that the College’s reaction will be proportionate and appropriate. Action taken will be according to Staff Disciplinary Procedures and the Bosworth Staff Code of Conduct as well as with reference to GDPR, safeguarding requirements (including the current versions of KCSIE and Working Together. See below.

Student Incidents	Refer to Head of Department / Year /	Refer to Principal / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Removal of network / internet access
Deliberately accessing or trying to access material that could be considered illegal as appropriate	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X				
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X	X			
Unauthorised / inappropriate use of social media / messaging apps / personal email (as appropriate)	X	X	X		
Unauthorised downloading or uploading of files	X	X		X	
Allowing others to access College network by sharing username and passwords	X				
Attempting to access or accessing the College network, using another student's / pupil's account	X				X
Attempting to access or accessing the College network, using the account of a member of staff	X	X		X	X
Corrupting or destroying the data of other users	X	X		X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X		X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X
Actions which could bring the College into disrepute or breach the integrity of the ethos of the College	X	X		X	X
Using proxy sites or other means to subvert the College's / academy's filtering system	X	X		X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X		X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X		X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the DPA	X	X			X

Staff Incidents	Refer to Principal	Refer to Local Authority /	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Appropriate disciplinary
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X
Inappropriate personal use of the internet / social media / personal email	X	X	X	X	X
Unauthorised downloading or uploading of files	X	X		X	X
Allowing others to access College network by sharing username and passwords or attempting to access or accessing the College network, using another person's account	X	X		X	X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X			X
Deliberate actions to breach data protection or network security rules	X	X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X		X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students	X	X		X	X
Actions which could compromise the staff member's professional standing	X	X		X	X
Actions which could bring the College into disrepute or breach the integrity of the ethos of the College	X	X		X	X
Using proxy sites or other means to subvert the College's / academy's filtering system					

Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X
Breaching copyright or licensing regulations	X	X		X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X