



Bosworth
Independent
School

Online Safety Policy

Reviewed	August 2025
Next Review Date	August 2026
Lead for Review	Assistant Head Pastoral

Contents

Key contacts	3
Introduction	4
Information on internet technology	4
Roles and responsibilities	4
Working with parents and carers	6
Teaching online safety	7
Content	7
Safe use of technology	8
Safety rules.....	9
Students own mobile devices	10
Policy statement	10
Unintentional access of inappropriate websites	11
Intentional access of inappropriate websites by a student	11
Action by service providers	12
Harmful sexual behaviour online	12
Risk from inappropriate contacts with adults	13
Risk from contact with violent extremists	13
Risk from sites advocating suicide, self-harm and anorexia.....	14
Appendix 1:	14
Online safety incident report form	14

Key contacts

Name of School/School: Bosworth Independent School**Headteacher:**

Name: Tony Oulton

Contact details: TOulton@Bosworthschool.co.uk

Online safety co-ordinator:

Name: Ita Coverdale

Contact details: ICoverdale@Bosworthschool.co.uk

IT Manager:

Name: Kieron Connelly

Contact details: KConnelly@catsglobalschools.com

Designated safeguarding lead:

Name: Ita Coverdale

Contact details: ICoverdale@Bosworthschool.co.uk

Nominated governor:

Name: Liz Francis

Contact details: LFrancis@catsglobalschools.com

West Northants County Council**Child protection lead officer and Local Authority Designated Officer (LADO):**

Name: Andy Smith

Contact details: ladoreferral@nctrust.co.uk / 01604 362993

Child and Family Contact/MASH team:

Tel: 0300 126 7000

<http://www.nctrust.co.uk/help-and-protection-for-children/Pages/report-a-concern.aspx>

Northants online safety and wellbeing officer:

Name: Simon Aston

Tel: 0300 126 7000 / 07841 784610

OnlineSafety.NCC@northnorthants.gov.uk

Prevent Education Officer

Name: Simon Aston

Tel: 0300 126 7000 / 07841 784610

OnlineSafety.NCC@northnorthants.gov.uk

Introduction

Information on internet technology

The educational and social benefits for students in using the internet should be promoted, but this should be balanced against the need to safeguard students against the inherent risks from internet technology. Further, Schools need to be able to teach children how to keep themselves safe whilst on-line. This is particularly important given that students predominantly access the internet through their own providers, which cannot be filtered.

Roles and responsibilities

A successful online safety strategy needs to be inclusive of the whole School community, including teachers, boarding staff, governors and others, and forge links with parents and the sales team. The strategy should be overseen by the Headmaster and be fully implemented by all staff, including operations and non-teaching staff.

Headmaster's role

Headmasters have ultimate responsibility for online safety issues within the School including:

- the overall development and implementation of the School's online safety policy and ensuring the security and management of online data
- ensuring that online safety issues are given a high profile within the School community
- linking with the board of governors and parents and sales team to promote online safety and forward the School's online safety strategy
- ensuring online safety is embedded in staff induction and training programmes

- deciding on sanctions against staff and students who are in breach of acceptable use policies and responding to serious incidents involving online safety.

Governors' role

Governing bodies have a statutory responsibility for student safety and should therefore be aware of online safety issues, providing support to the Headmaster in the development of the School's online safety strategy.

Governors should ensure that there are policies and procedures in place to keep students safe online and that these are reviewed regularly.

Governors should be subject to the same online safety rules as staff members and should sign an Acceptable Use Agreement in order to keep them safe from allegations and ensure a high standard of professional conduct. In particular, governors should always use business email addresses when conducting School business.

Online safety co-ordinator's role

The School should have a designated online safety co-ordinator who is responsible for co-ordinating online safety policies on behalf of the School. Ideally, the officer should be a senior member of the leadership team.

The online safety co-ordinator should have the authority, knowledge and experience to carry out the following:

- develop, implement, monitor and review the School's online safety policy
- ensure that staff and students are aware that any online safety incident should be reported to them
- ensure online safety is embedded in the curriculum
- provide the first point of contact and advice for School staff, governors, students and parents regarding how to keep safe online
- liaise with the School's IT manager, the Headmaster and nominated governor to ensure the School remains up to date with online safety issues and to address any new trends, incidents and arising problems
- assess the impact and risk of emerging technology and the School's response to this in association with IT Manager and learning platform providers
- raise the profile of online safety awareness with the School by ensuring access to training and relevant online safety literature
- ensure that all staff and students have read and signed the acceptable use policy (AUP)
- report annually to the board of governors on the implementation of the School's online safety strategy

The log of internet related incidents and co-ordination of any investigation into breaches will be maintained and led by the DSL.

IT's Manger's role

- the maintenance and monitoring of the School internet system including anti-virus and filtering systems
- carrying out monitoring and audits of networks and reporting breaches to the online safety co-ordinator
- supporting any subsequent investigation into breaches and preserving any evidence.

Role of School staff

All School staff have a dual role concerning their own internet use and providing guidance, support and supervision for students. Their role is:

- adhering to the School's online safety and acceptable use policy and procedures
- communicating the School's online safety and acceptable use policy to students
- keeping students safe and ensuring they receive appropriate supervision and support whilst using the internet
- planning use of the internet for lessons and researching on-line materials and resources
- reporting breaches of internet use to the online safety co-ordinator
- recognising when students are at risk from their internet use or have had negative experiences and taking appropriate action, for example referral to the online safety co-ordinator
- teaching the online safety and digital literacy elements of the new curriculum.

Designated safeguarding leads

Where any online safety incident has serious implications for the child's safety or well-being, the matter should be referred to the designated safeguarding lead for the School who will decide whether or not a referral should be made to Children's Safeguarding and Social Work or the Police.

Working with parents and carers

It is essential that the School involves parents and the student recruitment team in the development and implementation of online safety strategies and policies; most students will have internet access at home or own mobile devices and might not be as closely supervised in its use as they would be at the School.

Therefore, parents and the sales team need to know about the risks so that they are able to continue online safety education at home and regulate and supervise children's use as appropriate to their age and understanding.

The Headmaster, board of governors and the online safety coordinator should consider what strategies to adopt in order to ensure parents are aware of online safety issues and support them in reinforcing online safety messages at home.

Online safety policies

Teaching online safety

Responsibility

One of the key features of the School's online safety strategy is teaching students to protect themselves and behave responsibly while on-line. There is an expectation that over time, students will take increasing responsibility for their own behaviour and internet use so that they can be given more freedom to explore systems and applications with a lessening amount of supervision from staff.

- Overall responsibility for the design and co-ordination of online safety education lies with the Headmaster and the online safety coordinator, but all staff should play a role in delivering online safety messages.
- The online safety coordinator is responsible for ensuring that all staff have the knowledge and resources to enable them to carry out this role.
- Teachers are primarily responsible for delivering an ongoing online safety education in the classroom as part of the curriculum.
- The start of every lesson where computers are being used should be an opportunity to remind students of expectations on internet use and the need to follow basic principles in order to keep safe.
- The School is required to teach about online bullying as part of Relationships and Sex Education and health education.
- PSHE lessons provide an ideal for discussion on online safety issues to ensure that students understand the risks and why it is important to regulate their behaviour whilst on-line. This is to include educating all students about the potential harm around misinformation, disinformation and fake news.
- Teachers should be aware of those students who may be more vulnerable to risk from internet use, generally those students with a high level of experience and good computer skills but coupled with poor social skills for example students with SEND.
- Teachers should ensure that the School's policy on students' use of their own mobile phones and other mobile devices in School is adhered to. This includes boarding, classrooms and around the school site.

Content

Students should be taught all elements of online safety included in the computing curriculum so that they:

- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

- can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems.
- are responsible, competent, confident and creative users of information and communication technology.

Students should be taught all elements of online safety included in statutory Relationships and Sex Education:

- about different types of bullying (including cyberbullying), the impact of bullying, responsibilities of bystanders to report bullying and how and where to get help.
- their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- about online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- what to do and where to get support to report material or manage issues online.
- the impact of viewing harmful content.
- that specifically sexually explicit material e.g. pornography presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
- that sharing and viewing indecent images of students (including those created by students) is a criminal offence which carries severe penalties including jail.
- That making, posting or sharing pictures of nude or semi-nude of students (including themselves) online is a criminal offence.
- how information and data is generated, collected, shared and used online.

Statutory Health Education should include:

- the similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including through setting unrealistic expectations for body image, how people may curate a specific image of their life online, over-reliance on online relationships including social media, the risks related to online gambling including the accumulation of debt, how advertising and information is targeted at them and how to be a discerning consumer of information online).
- how to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support if they have been affected by those behaviours.

Safe use of technology

Internet and search engines

- When using the internet, students should receive the appropriate level of supervision for their age and understanding. Teachers should be aware that often, the most computer-literate students are the ones who are most at risk.
- Students should not be allowed to aimlessly “surf” the internet and all use should have a clearly defined educational purpose.
- Despite filtering systems, it is still possible for students to inadvertently access unsuitable websites; to reduce risk, teachers should plan use of internet resources ahead of lessons by checking sites and storing information off-line where possible.

- Where teachers require access to blocked websites for educational purposes, this should be discussed and agreed with the online safety coordinator, who will liaise with the IT team for temporary access. Teachers should notify the online safety coordinator once access is no longer needed to ensure the site is blocked.

Evaluating and using internet content

Teachers should teach students good research skills that help them maximise the resources available on the internet so that they can use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.

Safe use of applications

- **School email systems** should be hosted by an email system that allows content to be filtered and allow students to send emails to others within the School or to approved email addresses externally.
- **Social networking sites** such as Facebook, Instagram and Twitter allow users to publish information about them to be seen by anyone who has access to the site. Generally, these would have limited use in the School but students are likely to use these sites at home.
- **Online communities and forums** are sites that enable users to discuss issues and share ideas on-line.
- **Chat rooms** are internet sites where users can join in “conversations” on-line; **Instant messaging** allows instant communications between two people on-line. In most cases, students will use these at home although School internet systems do host these applications.
- **Gaming-based sites** allow students to “chat” to other gamers during the course of gaming. Many of the gaming sites are not properly moderated and may be targeted by adults who pose a risk to students. Consequently such sites should not be accessible via School internet systems.

Safety rules

- Access to and use of personal email accounts, unregulated public social networking sites, chat rooms or gaming sites on the School internet system is forbidden and is usually blocked. This is to protect students from receiving unsolicited mail or contacts and to preserve the safety of the system from hacking and viruses.
- If the School identifies a clear educational use for emails or social networking sites and forums for on-line publishing, they should only use approved sites such as those provided by the IT service provider. Any use of these sites should be strictly supervised by the responsible teacher.
- Emails should only be sent via the School internet system to addresses within the School system or approved external address. All email messages sent by students in connection with School business must be checked and cleared by the responsible teacher.
- Where teachers wish to add an external email address, this must be for a clear educational purpose and must be discussed with the online safety coordinator who will liaise with the learning platform provider.
- Student email addresses must not be published on the School website.
- Students should be taught to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender.
- Students should be taught not to disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence or on social networking sites.
- All electronic communications should be polite; if a student receives an offensive or distressing email or comment, they should be instructed not to reply and to notify the responsible teacher immediately.
- Students should be warned that any bullying or harassment via email, chat rooms or social networking sites will not be tolerated and will be dealt with in accordance with the School’s anti-bullying policy

and Safeguarding policy. This should include any correspondence or contact taking place outside the School and/or using non-School systems or equipment.

- Users should be aware that as use of the School internet system is for the purposes of education or School business only, and its use may be monitored.
- In order to teach students to stay safe online outside of School, they should be advised:
 - not to give out personal details to anyone on-line that may help to identify or locate them or anyone else, for example home address, name of School or clubs attended
 - to only use moderated chat rooms that require registration and are specifically for their age group;
 - not to upload personal photos of themselves or others onto sites and to take care regarding what information is posted as there is no control where images may end up or who can see them
 - how to set up security and privacy settings on sites or use a “buddy list” to block unwanted communications or deny access to those unknown to them
 - to behave responsibly whilst on-line and keep communications polite
 - not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken.
 - not to give out personal details to anyone on-line that may help to identify or locate them or anyone else
 - not to arrange to meet anyone whom they have only met on-line or go “off-line” with anyone they meet in a chat room
 - to behave responsibly whilst on-line and keep communications polite
 - not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken.

Students own mobile devices

The majority of students are likely to have mobile phones or other devices that allows them to access internet services, and these can pose a major problem for the School in that their use may distract students during lessons and may be used for online bullying. However, many parents prefer their students to have mobile phones with them in order to ensure their safety and enable them to contact home if they need to. Generally, use of personal mobile phones or other devices should be forbidden in classrooms. As a rule, mobile phones are to be handed in at the start of each lesson unless instructed otherwise by their subject teacher.

Responding to incidents

Policy statement

- All incidents and complaints relating to online safety and unacceptable internet use will be reported to the DSL in the first instance. All incidents, whether involving students or staff, must be recorded by the DSL on the online safety incident report form (appendix 1).
- Where the incident or complaint relates to a member of staff, the matter must always be referred to the Headmaster for action or consideration given to contacting the LADO where this is appropriate. Incidents involving the Headmaster should be reported to the chair of the board of governors.
- The School’s online safety coordinator should keep a log of all online safety incidents and complaints and regularly review the information for evidence of emerging patterns of individual behaviour or weaknesses in the School’s online safety system, and use these to update the online safety policy.

- Online safety incidents involving safeguarding issues, for example contact with inappropriate adults, cyberbullying should be reported to the designated safeguarding lead, who will make a decision as to whether or not to refer the matter to the police and/or Students Safeguarding and Social Work in conjunction with the Headmaster.

Although it is intended that online safety strategies and policies should reduce the risk to students whilst on-line, this cannot completely rule out the possibility that students may access unsuitable material on the internet. Neither the School nor the London Borough of Camden can accept liability for material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment.

Unintentional access of inappropriate websites

If a student or teacher accidentally opens a website that has content which is distressing or upsetting or inappropriate to the students' age, teachers should immediately (and calmly) close or minimise the screen.

Teachers should reassure students that they have done nothing wrong and discuss the incident with the class to reinforce the online safety message and to demonstrate the School's "no blame" approach.

The incident should be reported to the DSL and online safety coordinator and details of the website address and URL provided to the IT manager.

The online safety coordinator should liaise with the IT manager or learning platform provider to ensure that access to the site is blocked and the School's filtering system reviewed to ensure it remains appropriate.

Intentional access of inappropriate websites by a student

If a student deliberately accesses inappropriate or banned websites, they will be in breach of the acceptable use policy and subject to appropriate sanctions (see section 5).

The incident should be reported to the DSL and online safety coordinator and details of the website address and URL recorded.

The online safety coordinator should liaise with the IT manager or learning platform provider to ensure that access to the site is blocked.

The student's parents may be notified of the incident and what action will be taken.

The student will be reminded of the risks associated with such websites and material.

As part of online safety awareness and education, students should be told of the "no tolerance" policy for online bullying and encouraged to report any incidents to their teacher.

Students should be taught:

- to only give out mobile phone numbers and email addresses to people they trust.
- to only allow close friends whom they trust to have access to their social networking page.
- not to send or post inappropriate images of themselves

- not to respond to offensive messages.
- to report the matter to their parents and teacher immediately.

Evidence of bullying, for example texts, emails or comments on websites should be preserved by the young person as evidence.

Any action taken on online bullying incidents must be proportional to the harm caused. For some cases, it may be more appropriate to help the students involved to resolve the issues themselves rather than impose sanctions.

Action by service providers

All website providers and mobile phone companies are aware of the issue of online bullying and have their own systems in place to deal with problems, such as tracing communications. Teachers or parents can contact providers at any time for advice on what action can be taken.

- Where the bullying takes place by mobile phone texts, the mobile phone company can be contacted to ask them to trace the calls. The student should also consider changing their phone number.
- Where the bullying takes place by email, and the messages are being sent from a personal email account, contact the service provider so that the sender can be traced. The student should also consider changing email address.
- Where bullying takes place in chat rooms or gaming sites, the student should leave the chat room or gaming site immediately and seek advice from parents or teachers. Bullying should be reported to any chat room moderator to take action.
- Where bullying involves messages on social networking sites or blogs, contact the website provider to request that the comments are removed. In extreme cases, the bully's access to the site can be blocked.
- Parents should be notified of any incidents where appropriate and advised on what measures they can take to block any offensive messages on computers at home.

Harmful sexual behaviour online

The internet contains a high level of sexually explicit content and internet-based communications systems and social networking sites can be used to send sexually explicit messages and images. In some cases these actions may be harmful or abusive or may constitute harassment or online bullying.

Staff should be aware of online behaviours of a sexual nature that could constitute harmful behaviour:

- sharing explicit and unwanted content and images
- upskirting
- sexualised online bullying
- unwanted sexualised comments and messages
- sexual exploitation, coercion or threats.

Staff should be aware of the duty under statutory guidance *Keeping students safe in education* and *Sexual violence and sexual harassment between students in Schools* and Schools which requires the

School to have policies in place to deal with incidents of on-line sexual harassment. Staff should be aware to report these concerns to the DSL where this raises a concern.

Risk from inappropriate contacts with adults

Teachers may be concerned about a student being at risk as a consequence of their contact with an adult they have met over the internet. The student may report inappropriate contacts or teachers may suspect that the student is being groomed or has arranged to meet with someone they have met on-line.

School staff should also be aware of students being sexually abused on-line through video messaging such as Skype. In these cases, perpetrators persuade the young person concerned to carry out sexual acts while the perpetrator watches/records.

- All concerns around inappropriate contacts should be reported to the designated safeguarding lead.
- The designated safeguarding lead should discuss the matter with the referring teacher and where appropriate, speak to the student involved, before deciding whether or not to make a referral to Students Safeguarding and Social Work and/or the police.
- The police should always be contacted if there is a concern that the child is at immediate risk, for example if they are arranging to meet the adult after School.
- The designated safeguarding lead can seek advice on possible courses of action from Camden's online safety officer in Students Safeguarding and Social Work.
- Teachers will advise the student on how to terminate the contact and change contact details where necessary to ensure no further contact.
- The designated safeguarding lead and the online safety coordinator should consider notifying the student's parents of any concerns or incidents and where appropriate, arrange to meet with them discuss what action they can take to ensure their child's safety.
- Where inappropriate contacts have taken place using School IT equipment or networks, the online safety coordinator should make a note of all actions taken and contact the network manager or learning platform provider to ensure that all evidence is preserved and that an audit of systems is carried out to ensure that the risk to other students is minimised.

Risk from contact with violent extremists

Many extremist groups who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences and may be radicalised as a result of direct contact with online extremists or because they self-radicalise having viewed extremist materials online.

All staff have a duty under the Government's Prevent programme to prevent vulnerable young people from being radicalised and drawn into terrorism. The main mechanism for this is the Channel Panel, a multi-agency forum that identifies young people who are at risk and develops a support plan to stop the radicalisation process and divert them from extremism.

- Staff need to be aware of the School's duty under the Prevent programme and be able to recognise any student who is being targeted by violent extremists via the internet for the purposes of radicalisation. Students and staff should be warned of the risks of becoming involved in such groups and informed that accessing such websites is against School policies.

- The School should ensure that adequate filtering is in place and review filtering in response to any incident where a student or staff member accesses websites advocating violent extremism.
- All incidents should be dealt with as a breach of the acceptable use policies and the School's behaviour and staff disciplinary procedures should be used as appropriate.
- The designated safeguarding lead should record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the School and whether current School procedures are robust enough to deal with the issue.
- Where there are concerns that a young person is being radicalised or is in contact with violent extremists, or that their parents are and this is placing the child or young person at risk, Schools should seek advice and refer the young person to the MASH.

Risk from sites advocating suicide, self-harm and anorexia

Some internet sites advocate dangerous activities such as self-harming, suicide or anorexia. Other sites contain sexually explicit material or glorify risky and illegal behaviours like substance misuse.

Exposure to potentially harmful materials online may normalise the issue for young people and desensitise them to the harm. Most young people who visit these sites will not be adversely affected, but some vulnerable, less resilient young people may feel drawn to the sites which may trigger harmful or even fatal behaviours.

- The School should ensure that young people have an opportunity to openly discuss issues such as self-harming, suicide, substance misuse and anorexia as part of the PHSE curriculum.
- Pastoral support should be made available to all young people to discuss issues affecting them and to establish whether their online activities are an added risk factor
- Staff should receive the training needed to raise awareness of these issues so that they are able to identify those young people who are at risk, offer appropriate support and make appropriate referrals for help.

Appendix 1:

Online safety incident report form

Name of School/organisation:

Address:

Name of online safety coordinator:

Contact details:

Details of incident**Date happened:****Time:****Name of person reporting incident:**

If not reported, how was the incident identified?

Where did the incident occur?

- In School/service setting Outside School/service setting

Who was involved in the incident?

- child/young person staff member other (please specify)

Type of incident:

- bullying or harassment (online bullying
 deliberately bypassing security or access
 hacking or virus propagation
 racist, sexist, homophobic, transphobic, bi-phobic, religious hate material
 terrorist material
 online grooming
 online radicalisation
 child abuse images
 on-line gambling
 soft core pornographic material
 illegal hard core pornographic material
 other (please specify)

Description of incident

Nature of incident **Deliberate access**

Did the incident involve material being;

- created viewed printed shown to others
 transmitted to others distributed

Could the incident be considered as;

- harassment grooming online bullying breach of AUP

 Accidental access

Did the incident involve material being;

- created viewed printed shown to others
 transmitted to others distributed

Action taken **Staff**

- incident reported to Head teacher/senior manager
 advice sought from LADO
 referral made to LADO
 incident reported to police
 incident reported to Internet Watch Foundation
 incident reported to IT
 disciplinary action to be taken

- online safety policy to be reviewed/amended

Please detail any specific action taken (i.e.: removal of equipment)

- Child/young person**

- incident reported to Head teacher/senior manager
- advice sought from Students Safeguarding and Social Work
- referral made to Students Safeguarding and Social Work
- incident reported to police
- incident reported to social networking site
- incident reported to IT
- child's parents informed
- disciplinary action to be taken
- child/young person debriefed
- online safety policy to be reviewed/amended

Outcome of incident/investigation