BLOOMFIELD COLLEGIATE SCHOOL

E-Safety and Acceptable Use of the Internet Policy

Approved by the Board of Governors 20 June 2019

Content

E-Safety and Acceptable Use of the Internet Policy

1.

1.1 Rationale for the need for an e-safety and Acceptable Use of the Internet Policy

This policy represents Bloomfield Collegiate School's approach to ensuring that **e-Safety** (electronic safety) is embedded in the use by pupils and staff of devices that can access the Internet. E-Safety at Bloomfield:

- is concerned with safeguarding children and young people in the digital world;
- emphasises learning to understand and the use of new technologies in a positive way;
- focuses on education about the risks as well as the benefits, so that users feel confident online;
- aims to help pupils to develop safer online behaviours both in and out of school; and
- aims to help pupils recognise unsafe situations and know how to respond to risks appropriately.

1.2 What does the policy cover?

E-Safety covers not only Internet technologies but also any electronic communication via smart phones, tablets, laptops, or any wireless enabled technology. When the word "**Internet**" is used in this policy it refers to any online activity e.g. Email, Internet access, cloud storage or interaction with the Virtual Learning Environment (VLE).

The rapidly changing nature of the Internet and new technologies means that e-Safety is an ever growing and changing area of interest and concern. Bloomfield Collegiate School's e-Safety and Acceptable Use of the Internet Policy must reflect this by keeping abreast of the changes taking place. Bloomfield Collegiate has a duty of care to enable pupils to use online systems safely. **This policy will be reviewed on an annual basis.**

1.3 Links to other school policies

The e-Safety and Acceptable Use of the Internet Policy operates in conjunction with other school policies including; Safeguarding and Child Protection Policy and Positive Relationships and Anti-Bullying Policy. E-Safety at Bloomfield is built into the delivery of the curriculum. As ICT is a compulsory cross-curricular element of the revised curriculum, this policy is intended to ensure the safe acquisition, development and use by pupils of these skills at Bloomfield Collegiate School.

1.4 What is the Internet?

The Internet is an electronic information highway connecting computers all over the world and millions of individual subscribers. This global "network of networks" is not governed by any entity. This means that there are **no limits** or checks on the kind of information that is maintained by, and accessible to, the Internet. The educational value of appropriate use of information and resources located on the Internet is substantial, allowing for the efficient digital exchange of appropriate information between pupils, staff and parents.

1.5 What is a VLE?

A Virtual Learning Environment (VLE) is a range of educational resources, comprising information, forums, assessments and other online material provided to students as part of an online learning package. FRONTER is the current VLE in use at Bloomfield Collegiate School supported by C2K.

1.6 Why use the Internet?

Bloomfield Collegiate School encourages use by pupils of the rich information sources available on the Internet. Online resources offer a broader range of up-to-date resources to pupils (both those at school and those unable to attend school), provide an independent research facility, facilitate a variety of learning styles and abilities and encourage pupils to take responsibility for their own learning.

1.7 Networked access to Internet

In recognition of these benefits, Bloomfield Collegiate School offers networked Internet, VLE and email access to pupils and staff on the school network. Appropriate cross-curricular use of the Internet and the VLE is actively encouraged.

1.8 How will pupils gain access to the Internet and VLE at Bloomfield Collegiate School?

- In ICT specific lessons.
- Through non ICT subject use across the curriculum.
- During break and lunch times at various ICT resourced locations around the school.
- In lunch or after school clubs using ICT resourced locations.
- By using their own mobile device (tablet, laptop or smartphone) under certain conditions specified in section 11.

1.9 Use of pupil owned mobile Internet enabled devices

Under certain conditions (as outlined in section 11) Bloomfield Collegiate supports pupils using their own personal devices to further their learning. The opportunities to use the Internet and access online resources should not be restricted by access to school specific equipment.

Pupils have access to the secured network via the Wi-Fi network at school. **Pupils should understand that this policy applies equally to use of a school owned computer device and a pupil owned device when accessing networked material**.

In school, pupils are **strictly forbidden** to access Internet resources outside the school network such as those provided through phone 3G/4G contracts.

The use by pupils of mobile devices is only permitted within the school day through **instruction by the teacher** or by **teacher approved request** from the pupil. Where it states in this policy 'use by pupil of the Internet,' it applies both to school hardware or pupil owned devices during the school day.

Pupils are solely responsible for their own devices if being used at school. The school does not accept responsibility for damage or loss to these devices and it is the pupils' responsibility to ensure they are kept secure at all times.
Section 11 of this policy outlines guidelines relating to '**bring your own device'.**

1.10 Dangers in using the Internet

Since the Internet is composed of information from a vast array of sources worldwide, it includes some material that is not of educational value in the context of the school. This material includes information that may be inaccurate, abusive, sexually oriented, racist, sectarian or illegal. In order to guard young people from danger, it is the joint responsibility of school staff and the parent or guardian of each pupil to educate the pupil about her responsibility when using the Internet. The filtered C2K network provides protection to pupils and users, but, the nature of the Internet means that not all inappropriate material may be blocked. The schools' e-Safety and Acceptable Use of the Internet Policy is written in order to address these dangers and promote safe online use.

1.11 Promoting awareness of the e-Safety and Acceptable Use of Internet Policy

Bloomfield Collegiate School will endeavour to ensure that all stakeholders are made aware of this policy. The policy will be made available to parents, pupils, governors and staff. A copy will also be available on the website. The Principal will act as the Chair of the eSafety Group which will oversee eSafety training, policy and procedures. The group will consist of the Pastoral Vice Principal, ICT Coordinator and CEOP Ambassadors.

1.12 Policy compliance with DENI circulars

This policy has been created to support compliance with DENI circular 2011/22, 2013/15, 2016/26 & 2016/27

1.13 Approval steps in developing this policy

This policy has been jointly developed alongside Strathearn, Grosvenor and Sullivan Upper schools. It has had internal contributions from both staff and the school council.

Policy development

- eSafety Group
- Staff consultation.
- SLT consultation.
- School Council.
- Parental consultation.
- Board of Governors' approval.

2.0 Roles and Responsibilities

2.1 Pupils' responsibilities

Pupils are responsible for good behaviour on the Internet just as they are in the classroom, school corridor or school buses, so normal school rules will apply. In addition, a number of rules relating specifically to use of the Internet also apply.

Through the secured C2K network, Bloomfield Collegiate School has a filtered Internet and email service. Pupils are **not permitted** to use any other email service while at school. Internet, VLE and email services can be monitored and are not therefore private. Pupils are reminded that Internet, VLE activity and email messages can be viewed at any time.

2.2 Pupils' unacceptable behaviours

Misuse of the Internet is a breach of Bloomfield Collegiate Positive Behaviour and Citizenship policy and will incur the relevant sanctions. The following list applies to all uses of the Internet and mobile technologies including email, social media (Facebook, Instagram, Twitter, Snapchat etc), texting and messaging.

Examples of misuse of the Internet include the following. This list is not exhaustive.

- taking, retrieving, sending, copying or displaying impolite, discourteous or offensive images/text/messages/videos
- causing persistent irritation and/or wilful embarrassment to a member of the school community.
- send or play offensive sound recordings
- cause distress to another member of the school community
- making false allegations against others/written provocation against others.
- making racial, sectarian or homophobic comments
- harass, insult, bully or attack others
- refusing to follow teachers' instructions
- bringing the school into disrepute
- cheating
- damage or tamper with computers, computer systems or computer networks
- copying, saving and/or redistributing copyright protected material
- copy software from or to the school computer systems without prior permission from a teacher
- using the school computer systems to create or distribute malicious materials or software
- using the school computer systems to create or distribute software that could cause a security breach
- give out their C2K password to anyone
- use or attempt to use another user's password to access his/her network area
- trespass in another user's folders, work or files
- intentionally waste resources (such as consumables e.g. paper and toner)
- use the network for unapproved commercial purposes
- use ICT resources in any way that contravenes Health and Safety guidelines
- use any device to access the Internet unless access is through the C2K managed system
- take part in any form of cyberbullying
- subscribe to any services or ordering any goods or services, unless specifically approved by the school
- search or view materials that are not related to the curriculum or future careers
- play computer games or using other interactive 'chat' sites, unless specifically assigned by the teacher
- use the network in such a way that use of the network by other users is disrupted
- publish, share or distribute any personal information about a user
- carry out any activity that violates a school rule
- using or distributing by whatever means any material relating to school activities pupils or staff for which explicit permission has not been given
- engaging in any online activity that is harmful or hurtful to others, and
- taking or receiving pictures, videos, sound clips of pupils for which explicit permission has not been given by a teacher

2.3 Acceptable pupil behaviour

Online activities which are encouraged include, for example:

- use of the Internet to investigate and research school subjects, cross-curricular themes and topics;
- the use of email for communication between colleagues, between pupil(s) and teacher(s) between pupil(s) and pupil(s), between schools and industry;
- use of the Internet to investigate careers and further education;
- the development of pupils' competence in ICT skills and their general research skills.

2.4 Parental permission and responsibility

Access for the use of the Internet requires parental permission and a signed declaration by pupils agreeing to the school rules for use of the Internet.

This permission form is contained in **Appendix 2**

During class teachers will guide pupils towards appropriate materials. Outside school hours it is the responsibility of parents/guardians to provide guidance for information sources such as television, telephones, movies, radio, and other potentially offensive media.

2.5 Activities by pupils making reference to school name, staff members or pupils

Pupils should note that using or distributing via online mechanisms (including on social networking sites or similar) any material relating to school activities, pupils or staff for which explicit permission has not been given is unacceptable. This includes the posting of material, images or video footage relating to school staff, pupils, the school environment or school name. This applies to curricular and extra-curricular aspects of school life as well as to all school trips.

2.6 Action in the event of unacceptable behaviour by a pupil

If a pupil is discovered to be using the Internet in a way that it is deemed to have contravened this Acceptable Use of the Internet Policy, subsequent actions will follow the schools standard disciplinary procedure.

Serious breaches of non-permitted activities or concerns may result in local authority or PSNI involvement.

2.7 Action in the event of a pupil or member of staff being able to access/view inappropriate material online

If at any time a member of the school community finds that she/he is able to access, from within the school, Internet sites which are unsuitable or should be blocked she/he should close the site down and, in the case of a pupil, advise a staff member immediately. The staff member should report the incident as soon as possible to the Principal so that the site can be blocked (if appropriate) and the incident recorded in the Online Safety Register (Appendix 5).

2.8 Location and supervision of Internet based access

Internet access is available for pupils at Bloomfield at any networked computer around the school. This access may either be directly supervised (within a class) or not supervised (e.g. lunch or non-timetabled classes).

In addition pupils via the school Wi-Fi network can access the Internet within the range of the installed Wi-Fi system using their own network enabled device.

Pupils are reminded of their responsibility to use these resources in line with this policy.

Pupils are reminded that the school has the ability to review all files and online communications stored on the C2K network to ensure that the system is being used responsibly. While normal privacy is respected and protected by password controls, Internet users should not expect Internet and VLE activity, email or files stored on school servers to be private.

3.0 Acceptable use of digital photographs, images or videos of pupils

3.1 Parental consent for the taking of digital photographs or videos of pupils

Year 8 parents are issued with a letter requesting permission for photographs to be taken and displayed and an image of each child is taken for the computer system. The details of the parental response are held in the school office. Staff should check these details prior to image use.

Digital photographs or video may be taken at school activities and during the academic year and may be used, with parental consent, for display purposes in the school, for publication in the press or for promotional purposes.

For displays/use outside school or where staff require additional guidance on the display/use of photographs, the Senior Leadership Team should be consulted.

4.0 Training to support e-Safety

4.1 Pupil training

Bloomfield Collegiate School will endeavour to ensure that all pupils understand how they are to use the Internet, VLE and email appropriately and why the rules exist.

The Internet as a resource is provided for pupils to conduct research and communicate with others. While the use of information and communication technologies is a required aspect of the statutory Northern Ireland Curriculum, access to the Internet, VLE and email through C2K NI remains a privilege and not a right. It is given to pupils who act in a considerate and responsible manner, and will be withdrawn if they fail to maintain acceptable standards of use.

Child Exploitation and Online Protection (CEOP) resources are a useful teaching tool for all Key Stages looking at Internet safety. Pupil awareness training around Internet e-Safety issues is incorporated into the pupils' ICT programme of study. It is further supported through the schools pastoral programme. Training and support includes:

- specific e-Safety lessons - CEOPS training;
- guidance by individual teachers on safe Internet practice;
- reinforcement of e-Safety issues through the pastoral year programme.

4.2 External support resources

There are many appropriate resources now available in relation to Internet and e-Safety. These are available freely to parents and pupils. Childnet, as an example, has produced many materials to support the teaching of e-Safety at different key stages. They have also produced materials for parents, staff and post primary pupils. Websites to look at include *www.childnet.com, www.ceop.police.uk/,*
www.internetmatters.org, www.kidsmart.org.uk/beingsmart, www.thinkuknow.co.uk

5.0 Risk assessments

Bloomfield Collegiate will perform risk assessments on the technologies within the school to ensure that it is aware of and, mitigates against, the potential risks involved with their use.

5.1 Risk assessment process

Any teacher wishing to access a blocked website (by C2K) will be required to carry out a risk assessment on that website. The completed form (appendix 4) must be sent for approval to the curriculum VP at Bloomfield Collegiate who will make the final decision on authorization. All risk assessments will be filed in order to support the teaching and learning process at Bloomfield, and to develop best practice around the use of the Internet and associated technologies.

When making a request to unblock a website, teachers should remember that:

- the sites that are made available may contain inappropriate material;
- as the sites will only be available to staff, it is important to emphasize that a computer, on which a member

of staff has logged on, should not be left unattended;

- particular care should also be taken when accessing the sites while projecting the computer desktop on a whiteboard, as inappropriate material may be openly displayed.

6.0 Cyber bullying

Bloomfield Collegiate School takes cyber bullying very seriously. This form of bullying is considered within its anti-bullying policy and pastoral programme as well as within this policy.

Teachers are to be aware that social media sites can offer much with regards to teaching and learning experiences for the pupils, but that they bring their own unique issues and concerns.

Each social media technology that is to be utilised, should be risk assessed by teachers in the context of each school situation. Risk assessment form (appendix 4) should be completed before the use of a social media site is authorized in a classroom context.

6.1 Forms that cyber bullying can take.

- Email – nasty or abusive emails which may include viruses or inappropriate content.
- Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.
- Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user's profile.
- Online Gaming – abuse or harassment of someone using online multi-player gaming sites.
- Mobile Phones – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people.
- Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.
- Using any form of technology to blackmail or extort.

6.2 External information for cyber bullying

Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator. Pupils are reminded that cyber-bullying can constitute a criminal offence. While there is no specific legislation for cyber-bullying, the following may cover different elements of cyber-bullying behaviour:

- Protection from Harassment (NI) Order 1997
  http://www.legislation.gov.uk/nisi/1997/1180
- Malicious Communications (NI) Order 1988
  http://www.legislation.gov.uk/nisi/1988/1849
- The Communications Act 2003
  http://www.legislation.gov.uk/ukpga/2003/21

6.3 What to do if pupils feel they are being cyber bullied

Pupils are encouraged to report incidents of cyber-bullying to both the school and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases.

Bloomfield Collegiate School records all instances of cyber-bullying incidents to monitor the effectiveness of their preventive activities, and to review and ensure consistency in their investigations, support and sanctions.

7.0 Email and Internet security

7.1 Email Security

Staff and pupils are advised to only use the school C2K email system. The C2K filtering system provides both security and protection to C2K email accounts. At Bloomfield no other email system is approved for use by staff or pupils. Staff and pupils must be vigilant to the threat of fraudulent emails. **PIN numbers and passwords must not**

be sent via email. Any suspected fraudulent emails should not be opened and their existence reported to the Principal.

7.2 Internet Security

The access to the Internet via the C2K Education Network requires authentication using a C2K username and password. All access to the C2K network is then filtered via the C2K Education Network solution.

It is noted that all access via this network is fully auditable and reports of usage are available to the school principal.

7.3 Non C2K equipment

Use or access to the network via non C2K connections is not permitted at Bloomfield under any circumstances.

8.0 Policy review

This policy is to be **reviewed annually**. This review calendar reflects the rapidly changing nature of the Internet and associated technologies. Any changes to the eSafety and Acceptable Use of the Internet Policy are to be outlined in annual updates to pupils, staff, governors and parents.

9.0 User adherence to the e-Safety and Acceptable Use of the Internet Policy

As this policy is reviewed **every year**, any review considered significant should be supported by a signed declaration from all users.

In Year 8, and for new pupils, a signed acceptable user policy declaration is to be completed (see Appendix 2)

10.0 Information for Parents and pupil consent forms

Parents are informed in writing of the schools e-Safety and Acceptable Use of the Internet Policy. They are asked to give permission for their children to use the Internet. Pupils are also required to sign an undertaking agreeing to their proper use of the Internet.

10.1 Guidance for parents with Internet access at home

It is strongly advised that a home computer/mobile device with Internet access should be situated in a location where parents can monitor access to the Internet. Computers should be fitted with suitable anti-virus, antispyware and filtering software.

Parents should discuss with their children the school rules for using the Internet and implement these at home. Parents and children should decide together when, how long, and what comprises appropriate use.

Parents should become familiar with the sites their children visit, and talk to them about what they are learning.

Parents should use appropriate Internet filtering software for blocking access to inappropriate materials.

Parents should consider carefully whether children should have access to social networking sites e.g. facebook and what restrictions are needed to ensure safe use of such sites.

Parents should ensure that they give their agreement before their children give out personal information in any electronic communication on the Internet, such as a picture, an address, a phone number, the school name, or financial information such as credit card or bank details. In this way they can protect their children (and themselves) from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud.

Parents should encourage their children not to respond to any unwelcome, unpleasant or abusive messages, and to tell them if they receive any such messages or images. If the message comes from an Internet service connection provided by the school or by C2K, they should immediately inform the school.

Further free advice for parents is available from the following sources:

www.thinkuknow.co.uk
www.kidsmart.org.uk
www.getnetwise.org

11.0 Pupils bringing their own device to school

11.1 Request and Instruction

During the school day the use of devices owned personally by pupils is subject to the same requirements as technology provided by the school. Bloomfield Collegiate recognises the opportunities that exist for pupils to actively learn through using their own device at school. It supports their use within the learning context with the understanding that controls must be put in place for their safe use.

The rules governing pupils using their own devices are either by **REQUEST** from the pupil or **INSTRUCTION** from the teacher.

REQUEST

In this situation, the pupil makes a request that she use her own device to access the Internet or use the device to further her learning in the classroom or at school. The teacher responds to this request by the pupil for the duration of that lesson only.

INSTRUCTION

The teacher gives instruction as appropriate for pupils to use their own device.

11.2 Conditions for pupils using their own devices

1. The device must be used in accordance with the e-Safety and Acceptable Use of the Internet Policy.
2. Any inappropriate content stored on the device in breach of the e-Safety and Acceptable Use Policy must be removed before it is brought into the school premises.
3. Pupils should have an up-to-date anti-virus/Internet security product on their device.
4. Acceptance that the school **takes no responsibility** for any device brought into school.
5. Parents/Guardians should have appropriate insurance measures in place to cover the device for this application.
6. The pupil is solely responsible for the safety (including content) of the device on his/her way to school, during school and on the return from school.
7. Use of the Internet and email is monitored and, any use deemed to be inappropriate, will be dealt with using the school’s disciplinary procedures and policies.
8. If a teacher suspects school rules have been broken, pupils can be asked to display images stored on their device.
9. If inappropriate and/or illegal materials are discovered, then the incident will be pursued through the schools’ disciplinary procedure.
10. There should be no use of cameras (if available on the device) to take images or video of pupils or a staff member without explicit staff and pupil permission.
11. Pupils who wish to connect their personal equipment to the school wireless network, should have no expectations of hardware or software support from the school.
12. Devices should be named ideally with a UV pen in accordance with advice from the police.
13. Pupils will be responsible for the security of their passwords and if their device is left unattended, the pupil should have either logged off or locked the device to prevent anyone using it in their absence.

14. If a pupil suspects that her device has been affected by a virus or other malware, it should be removed from the school network and fixed before using on the school network again.

15. Any charging device brought to school must be available for PAT testing to ensure electrical safe compliance.

Pupils and parents should also note:

- Pupils should be conscious of personal safety when carrying devices to, around and from school.

- Pupils should be conscious of personal safety when communicating online, and therefore will not share unnecessary personal information about themselves or others.

- It is also the user's responsibility to ensure that, where possible, devices brought in to school have an up-to-date anti-virus/Internet security program that receives regular updates. Failure to do so may result in viruses being transferred to school computers via email, removable storage devices or by access to the school folders remotely.

11.3 Agreement to guidelines "bring your own device"

To enable pupils to use their own device at school, under the terms of the e-Safety and Acceptable Use of the Internet Policy, written permission is required. Parents/guardians should sign and return the permission form for pupil Internet access and bring your own device Appendix 2

12.0 Online Safety Risk Register

12.1 Rationale

DENI Circular 2016/27 recommends that an Online Safety Risk Register is maintained to keep an up-to-date record of potential breaches of online safety. Potential breaches will include access to inappropriate sites, fraudulent emails, inappropriate use of email with internal or external users and inappropriate use of social media. This is not an exhaustive list.

12.2 Procedure

If pupils or staff suspect that there has been a breach of online safety the Principal will be informed as soon as possible. The Principal will take the appropriate actions such as blocking an inappropriate site, using existing school policies (safeguarding, pastoral and discipline) to investigate the breach and informing statutory agencies, if appropriate. The Online Safety Risk Register will be completed.

Reviewing Committee: Education Committee

Date Review Completed	Nature of Change	Date Ratified by Board of Governors
December 2014	New Policy	26 February 2015
February 2016	No changes	21 April 2016
February 2017	Minor changes	23 February 2017
June 2018	Minor Changes	14 June 2018
May 2019	Minor name change	20 June 2019

Dear Parent/Guardian,

e-Safety and Acceptable Use of the Internet Policy – Permission form

As part of the school's ICT strategy, Bloomfield Collegiate offers pupils access to a filtered Internet service. Before being allowed to use the Internet, all pupils must obtain parental permission and both they and you must sign and return the enclosed form as evidence of your approval and their acceptance of the school rules on Internet access and use.

Access to the Internet will enable pupils to explore thousands of libraries, databases, and bulletin boards while exchanging messages with other Internet users throughout the world. Families should be warned that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

Whilst our aim for Internet use is to further educational goals and objectives, pupils may find ways to access other materials as well. We believe that the benefits to pupils from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. We have put in place a filtered Internet and e-mail service to minimise the dangers of pupils gaining access to unsuitable materials. In addition, a clear set of rules and procedures for pupil use of the Internet has been implemented. Ultimately, however, parents and guardians are responsible for setting and conveying the standards that their children should follow when using media and information sources.

During class, teachers will guide pupils towards appropriate materials. Clear rules and procedures are in place for proper use of the Internet. Outside of school, families must bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio and other potentially offensive media. Appropriate home use of the Internet by children can be educationally beneficial and can make a useful contribution to home and school work. It should, however, be supervised, and parents should be aware that they are responsible for their children's use of Internet resources at home.

Whilst we endeavour to continue to educate in this challenging area, pupils are only permitted to access online materials using Internet connections provided and filtered by, or on behalf of, Bloomfield Collegiate School. We appreciate your ongoing support as we work together to ensure the safety of your child and those in our wider school community.

Free eSafety advice is widely available on the Internet, examples include: from the following sources:
http://www.thinkuknow.co.uk/ - a website designed to inform children of the potential hazards involved with online chatrooms.
http://www.parentsonline.gov.uk/ - promotes home school links by helping parents understand the role of ICT in learning
http://www.getnetwise.org/ - information about filtering programs for home use
We would be grateful if you could read the enclosed guidance documents and then complete the permission form which follows.

Yours sincerely

____

G. Greer Principal

Appendix 1

Bloomfield Collegiate Pupil Internet Access and 'Bring Your Own Device' Consent Form

Please complete and return this form to enable your daughter to access the Internet at school. The form also authorizes your daughter to bring her own device to school and for her to use the device within the terms as outlined in the e-Safety and Acceptable Use of Internet Policy.

By signing this form you:

1. Have read and understood the e-Safety and Acceptable Use of the Internet Policy and agree to abide by this policy
2. Confirm that a device brought to school by your daughter will **only be used in** accordance with this policy
3. Confirm that you accept full responsibility for the full replacement value of all electronic equipment which the pupil mentioned below brings into school.
4. Understand that the school's Internet services are filtered in an effort to prevent pupils from coming into contact with objectionable material; however incidents may still occur when inappropriate material has not been blocked by the filtering service.
5. Understand that your daughter must comply with Bloomfield Collegiate School's e-Safety and Acceptable Use of the Internet Policy and support the sanctions that are outlined in the schools disciplinary policy.

This contract will remain in force **throughout the pupil's time** at school and may be revised to take account of technological advancements in the interests of pupil safety. Return the signed form to the school office/form teacher.

As the parent or legal guardian of the pupil below, I **grant permission** for my daughter to use the Internet and bring her own device to school.

Parent's/Guardian's Agreement

NAME of Pupil: ________________________________ (Please Print)

Signed Parent/Guardian: ____________________________ Date: _______________

Pupil's Agreement

I have read and understand the Pupils' Roles and Responsibilities (Section 2.0) & Guidance for Pupils on the use of the Internet (Appendix 3). I will use the computer system, including my own devices, in a responsible way and obey the school rules at all times.

Signed Pupil: ____________________________ Date: _______________

The information on this form is covered by the provisions of the Data Protection Act, 1998. Your signature on the form is deemed to be an authorization by you to allow the School to process and retain the information for the purpose(s) stated

Appendix 2

Guidance for pupils on the use of the Internet

Bloomfield Collegiate School encourages use by pupils of the rich information sources available on the Internet and the schools virtual learning environment (Fronter). Online resources offer a broader range of up-to-date resources to pupils; provide an independent research facility; facilitate a variety of learning styles and abilities and encourage pupils to take responsibility for their own learning.

Access to the Internet, email and online resources is a privilege, not a right and this facility must be used responsibly. Parental consent and permission is required. All individual users are responsible for their behaviour and communications over the network. It is presumed that pupils will comply will school standards and the agreements they have signed.

Guidelines for pupils:

- Passwords are private and should **not** be given out under any circumstance
- **Do not publish** in any form another pupils **personal details** (including images) via Fronter/Internet or email
- **Any files** downloaded/uploaded **should not** offend or **be inappropriate** in any way
- Help protect yourself by **informing teachers** of any **inappropriate communications** you receive whilst online or using the Internet
- **Do not damage** or interfere in any way with the schools fixed or mobile computer equipment. This includes **not drinking/eating** whilst using the school's computer equipment
- **Any damage** discovered to the school's computer equipment should be **notified to a teacher** or a member of school staff
- Do not attempt to **open/copy/change** or delete **another pupil's files**

The following are **NOT** permitted and are **UNACCEPTABLE**:

- retrieve, send, copy or display offensive messages or pictures;
- send or play offensive sound recordings;
- use obscene or racist language;
- harass, insult, bully or attack others;
- damage or tamper with computers, computer systems or computer networks;
- violate copyright laws;
- copy software from the school computer systems;
- copy computer software, including computer games on to the school systems;
- give out their C2K password to anyone;
- use or attempt to use another user's password to access his/her network area;
- trespass in another user's folders, work or files;
- intentionally waste resources (such as consumables e.g. paper and toner);
- use the network for unapproved commercial purposes;
- use ICT resources in any way that contravenes Health and Safety guidelines;
- use any device to access the Internet unless access is through the C2K managed system;
- any form of cyberbullying.

For information about personal safety when online please refer to

- www.thinkuknow.co.uk
- www.childnet.com
- www.kidsmart.org.uk

Appendix 3

Request to unblock website RISK ASSESSMENT form

Intended year group /pupils ____________________

Website address ____________________

Date of request ____________________

Duration that website is to be unblocked ____________________

Is the site for sole use of teacher/teachers? YES / NO

Is the site for use by pupils? YES / NO

Content of website
Explain educational value in allowing access to website/forum below

Risk assessment
From a review of the website state the risks associated with the website and steps that will be taken to minimize these risks to ensure safety of pupils

As the teacher requesting access to this site, I understand that:

- The site requested may contain inappropriate material as it exceeds the thresholds of our school filtering solution.
- For sites made available to staff only:
  - it is especially important to ensure that a computer on which the member of staff has logged on should not be left unattended
  - particular care should be taken while projecting the sites on a whiteboard, as inappropriate material may be displayed.

Teacher's Signature: ____________________

Authorized by: ____________________
(Curriculum VP)

Date: ____________________

This form should be passed to the curriculum VP

Appendix 4

Online Safety Risk Register

This register is completed by the Principal or designated deputy when a suspected online safety breach has occurred.

Date	Suspected Online Safety Breach	Actions Taken	Who?

Appendix 5