BLOOMFIELD COLLEGIATE SCHOOL

E-Safety and Acceptable Use of the Internet Policy

Approved by Board 26 February 2026

Contents **Page**

SECTION 1: GENERAL INFORMATION

RATIONALE

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. ICT as a compulsory cross-curricular element of the revised curriculum, and e-safety considerations must be built into this delivery.

E-safety at Bloomfield:

- is concerned with safeguarding children and young people in the digital world;
- emphasises understanding how to use technologies in a positive and safe 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 behaviors both in and out of school; and
- aims to help pupils recognise unsafe situations and know how to respond to risks appropriately.

This policy has been created to support compliance with DENI circular 2007/01 (acceptable use of the internet), 2011/22 (online safety), 2016/26 (effective educational use of digital devices) & 2016/27 (online safety).

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.

The internet is not governed by any one agency. This means that there are no limits or checks on the kind of information that can be accessed. The educational value from the resources available on the internet is substantial and allows for the efficient digital exchange of appropriate information between pupils, staff, and parents. Bloomfield Collegiate School encourages use by pupils of this rich information source. Online resources offer a broad range of up-to-date resources to pupils (both those at school and for those unable to attend school or through periods of remote learning), provide the option of independent research, facilitate a variety of learning styles and abilities, and encourage pupils to take responsibility for their own learning. In recognition of these benefits, Bloomfield Collegiate School offers networked internet through the MySchool portal to pupils and staff. Digital learning is encouraged wherever possible to enhance the curriculum. The school will adopt the new Department of Education network for 2025/26 and the same rules will apply to its use. The name C2k will change during –2025/26 academic year.

Since the internet is composed of information from a vast array of sources 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. 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 to address these dangers and promote safe online use.

It is the responsibility of the school, governors, staff, and parents to mitigate the risk associated with pupils using the internet through appropriate planning and actions. The E-Safety Policy outlines how Bloomfield intends to do this, helping ensure pupils stay safe when they are online.

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 Policy must reflect this by keeping abreast of the changes taking place. The UK Online Safety Act 2023 is designed to make the internet safer, particularly for children and vulnerable users, by regulating online content and holding tech companies accountable for harmful material. It is still yet to be fully understood where there may be gaps in regulation to protect children and young people from possible harm caused by AI. Ofcom is the online safety regulator in the UK and is responsible for publishing codes of practice and guidance on how companies can comply with their duties.

There is currently little in the way of specific legislation regarding the use of AI in schools, but guidance has been developed and is being regularly updated as the technology evolves. This policy will be reviewed on an annual basis in light of changing technology and guidance.

PURPOSE

The purpose of this policy is to:

- ensure the safety and wellbeing of pupils at Bloomfield is paramount when they use the internet to support their learning;
- provide pupils, staff and parents with the principles that should guide their approach to online safety.

CRITERIA FOR SUCCESS

The workings of the approaches outlined in this policy to support E-Safety will be successful if a strategy is implemented that includes:

- A structured e-Safety training program is in place for pupils at all key stages;
- Teachers and Non-Teaching staff taking part in E-Safety awareness training on a regular basis;
- An eSafety Group is established consisting of the Principal, Senior Leader with responsibilities for Safeguarding, Designated Teacher, Head of ICT, Digital Leader and CEOP Ambassador/s;
- A pupil eSafety Team is established led by the Head Girl, supported by the Digital Leader;
- Regular pupil, teacher and parent voice surveys addressing e-safety at school;
- Monitoring the sanctions that are applied when incidents connected to e-safety have arisen;
- E Safety Newsletter sent to parents Monthly and visible on school website;
- An annual review by Governors of this E-Safety and Acceptable Use of the Internet Policy.

SECTION 2: ROLES AND RESPONSIBILITIES

THE BOARD OF GOVERNORS

The Board of Governors are charged with promoting the welfare of pupils and protecting the pupils from abuse. To support this, they will:

- Review the schools E-Safety and Acceptable Use of the Internet Policy on an annual basis;
- Promote safe and acceptable working when using the internet for all staff and pupils;
- Have oversight of the operations of the E-Safety policy.

THE PRINCIPAL

The Principal will:

- Have overall responsibility for E-Safety across the school;
- Chair the E Safety Group which will oversee e-safety training, policy, and procedures.

C2K/CAPITA

Bloomfield uses a managed system which is maintained by C2k through Capita. They will ensure that:

- All equipment is maintained safely;
- Access to equipment is restricted to only those authorised to use it;
- All users are provided with username and password;
- Internet access is filtered;
- Personal data is encrypted.

STAFF

Teaching and Non-Teaching staff will:

- Contribute to the development of E-Safety Policies and procedures;
- Raise e-safety issues or apply good practice where appropriate;
- Adhere to the School E-Safety Policy and Acceptable Use Policies;
- Sign and return the Agreement Form appended to any relevant Acceptable Use Policy (Appendix 5);
- Have an awareness of e-safety matters and how they relate to pupils;
- Model good practice in using new and emerging technologies;
- Embed e-safety education in curriculum delivery where possible;
- Report any concerns to the Designated Teacher for E-Safety;
- At all times adhere to the School Code of Conduct for Staff and Volunteers.

PUPILS

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.

When using the internet at school pupils should:

- Follow the training given for using the internet around taking responsibility for being safe online, respecting the feelings and rights of others and assessing the personal risks of using a particular technology;
- Report any concerns around internet safety to an appropriate member of staff;
- When communicating digitally, do so in a professional tone;
- Not access the internet outside the controls of C2k whilst in school unless with the permission of the teacher.
- Sign the Pupil Acceptable Use Agreement Form to confirm they have read and understood the Acceptable Use Policy (Appendix 6);

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, Roblox, Minecraft, Snapchat, TikTok, Whats App 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;
- taking or receiving pictures, videos, sound clips of pupils for which explicit permission has not been given by a teacher.

Unacceptable behaviour by a pupil

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.

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 school's standard disciplinary procedure.

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

PARENTS

Parents should:

- Be aware of and understand the rationale behind the school's E-Safety Policy;
- Encourage their children to adhere to the policy through discussion and conversation;
- Support their children by encouraging them not to respond to any unwelcome, unpleasant, or abusive messages, and to tell them if they receive any such messages or images;
- Take an interest in what their children are doing online and discuss their online learning with them;
- Lead by example when using the internet and new technologies;
- Be responsible around what social media sites their children use and the legal restrictions to using these sites;
- Reinforce appropriate safe online behaviour at home;
- Ensure that pupils at home devices are situated where they can monitor, and that they have suitable anti-virus type software installed;
- Sign the parental permission for their child to use the internet (Appendix 1)

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

SECTION 3: EDUCATION, TRAINING AND SUPPORT

PUPIL TRAINING

Bloomfield Collegiate School will endeavour to ensure that all pupils understand how they are to use digital technologies in a safe and appropriate way. 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 online resources 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 school's pastoral programme. Training and support include:

- specific e-safety lessons - CEOP training;
- guidance by individual teachers on safe internet practice;
- reinforcement of e-safety issues through the pastoral year programme.

Safer Internet Week

During the annual Safer Internet Week, the eSafety Student Team, led by the Head Girl, delivers a selection of eSafety based activities to the pupils in KS3. This reinforces the material the pupils receive from other sources.

External eSafety Resources

These include websites and Apps. Parents, pupils and staff are encouraged to download the "saferschoolsNI App". This provides a digital library of age-appropriate safeguarding resources which is financed by the Department of Education for schools in Northern Ireland.

Websites
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 include:
www.childnet.com;
www.ceop.police.uk/;
www.internetmatters.org;
www.thinkuknow.co.uk;
www.saferinterent.org.uk;
www.nspcc.org.uk;
https://saferschoolsni.co.uk/;
Safety and Security Online | SWGfL;
www.Swiggle.org.uk – Child Suitable Search Engine.

EDUCATION OF PARENTS

Education of parents
The School recognises that parents have an essential role to play in enabling their daughter(s) to become safe and responsible users of the internet and digital technology. Parents' attention will be drawn to the Schools E-Safety Policy and expectations. Information and guidance for parents on online safety will be made available in a variety of formats, e.g. E-safety Newsletter (Monthly). Parents will be encouraged to model positive behaviour for their daughter(s) online. Parents are strongly encouraged to have regular conversations with their daughter(s) about the benefits and dangers of the Internet, to empower them to use the Internet safely.

RISKS ASSOCIATED WITH USING NEW TECHNOLOGIES

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.

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 3) must be sent for approval to the Vice-Principal at Bloomfield Collegiate who will make the final decision on authorisation. All risk assessments will be filed 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, projector or smart TV as inappropriate material may be openly displayed.

Digital images 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.

MOBILE PHONES

The School recognises that many parents may wish their daughter to have a mobile phone for use in cases of emergency. However, mobile phones can be used inappropriately, and they are potential targets for theft and online bullying-type behaviour. The School reserves the right to confiscate a pupil's mobile phone and retain it at Reception until 3.20 pm, should a pupil fail to co-operate with the arrangements outlined below.

Pupils will need to sign for their phones to retrieve them. Pupils who persistently fail to adhere to these arrangements will be disciplined in accordance with the School's Positive Behaviour Policy.

The use of mobile phones is restricted before Registration and after 3.20pm.
Phones must be SWITCHED OFF AT ALL OTHER TIMES, including between classes, unless directed otherwise by staff. The misuse of mobile phones and other personal electronic communication equipment for online bullying-type behaviour will not be tolerated (see Anti-Bullying, Positive Behaviour, Internet Acceptable Use).

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 3) should be completed before the use of a social media site is authorized in a classroom context.

Forms that cyber bullying may 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.

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.

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.

SECURITY

Email security
Staff and pupils are required to only use the school C2K email system when carrying out school business. The C2K filtering system provides both security and protection to C2K email accounts, and tracks email chains.

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

Data security
Data will be recorded, processed, transferred, and made available according to General Data Protection Regulations (GDPR). All users will be informed not to share passwords with others and not to login as another user at any time. Staff and pupils must always keep their passwords private and must not share them with others or leave it where others can find them. All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their passwords private.

Filtering
The School uses a filtered Internet and email service provided by C2K. The system is designed to filter sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc. If a member of staff or pupil should unwittingly discover an unsuitable site, the URL should be reported to the Digital Leader or the Designated Teacher for e-safety. This will then be recorded and escalated as appropriate to C2K. Any deliberate access to prohibited/unsuitable sites (within School or using a School-owned device) will be dealt with, as appropriate, according to the school's policies on Pupil Positive Behavior or acceptable use by for Staff and Volunteers.

Applications and Software used to Record Pupil Information
The Principal is ultimately responsible for the security of any data or images held of pupils. Apps/systems which store personal data will be assessed prior to use. Only School issued or sanctioned devices will be used for apps that record and store pupils' personal details, attainment, or photographs. Devices will be appropriately protected if taken off site to prevent a data security breach in the event of loss or theft.

SECTION 4: PUBLISHED CONTENT

School Website

The contact details on the website will be the School address, email and telephone number. Staff or pupils' personal information will not be published. While the Principal may delegate the day-to-day operation of the website, the Principal will take overall editorial responsibility for online content published by the School and will ensure that content published is accurate and appropriate. The School website will comply with the School's current policy and guidelines for publications including use of pupils' images, respect for intellectual property rights, privacy policies and copyright.

Publishing images and videos online

Use of images and video is an increasingly important element in modern educational practice. Videos can be produced by staff or pupils for a variety of educational purposes as well as for promotion and recording of activities. Images and videos may in some circumstances be published to an external storage or video sharing website. Where this is the case, current school guidelines on the use of these facilities will be followed by pupils and staff. The School will ensure that written permission from parents has been obtained before images/videos of pupils are electronically published.

Managing Email

The School will provide all pupils and staff with at least one official email address. These addresses are the only ones which should be used for school communication and educational purposes. School email can be monitored by senior staff. Pupils and staff will be made aware of the appropriate use of email and the sanctions if they abuse the email system. They will also be advised to be careful regarding with whom they share this email address. Pupils will be advised that this email address should only be used for school related activities and that it is not private. These addresses may be used to allow pupils to access services which the School has sanctioned, as appropriate, for use within school (e.g. cloud-based storage and associated applications). Use of email accounts and any services accessed using that account will only be used in accordance with the current school guidelines.

Official school Use of social media

Official social media used by the School will be in line with existing policies, including Anti-Bullying, Safeguarding and Child Protection. Images or videos of pupils will only be shared on official school social media sites/channels in line with the guidelines on image use which can be found in our Safeguarding and Child Protection Policy. Social media use will be age appropriate. The School is aware that many social media sites state that they are not for children under the age of 13, therefore the School will not create accounts within School specifically for pupils under this age. Information about safe and responsible use of School social media channels will be communicated clearly and regularly to all members of the School community.

The Principal and Designated Teacher for E-safety must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence. Parents and pupils will be informed of any official School social media use, along with expectations for safe use and School action taken to safeguard the community.

Where social media is used as part of a lesson or other educational experience this will be under the control of a member of staff. Staff discretion is advised and should be in line with the current guidelines and the Staff Code of Conduct. Official use of social media sites by the School will only take place with clear educational or engagement objectives with specific intended outcomes e.g. revision forums or increasing parental engagement. Staff use of social media sites as communication tools will only be used with permission of the Principal. School social media channels will be set up as distinct and dedicated social media site or accounts.

School social media accounts will be sanctioned by the Designated Teacher for E-Safety and will be set-up and managed by a member of School staff. Staff will use School provided email addresses to register for, and manage, official School approved social media channels. Members of staff running official School social media channels must ensure that they obtain prior permission from the Principal/Vice-Principal, are aware of the required behaviour and expectations of use and will monitor the use of the channel(s) to check they are being used safely, responsibly and in accordance with local and national guidance and legislation. All communication on official School social media platforms will be clear, transparent, and open to scrutiny. Any online publication on official School social media sites will comply with legal requirements including GDPR, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information, and will not breach any common law duty of confidentiality or copyright.

Staff will not engage with any direct or private messaging with pupils or parents through Private social media accounts and should communicate via recognised School communication channels. Any concerns regarding the online conduct of pupils, parents, or staff on social media sites should be reported to the Designated Teacher for E-safety or Designated Teacher for Child Protection and will be managed in accordance with existing School policies such as Anti-Bullying, Staff Code of Conduct, Safeguarding and Child Protection.

SECTION 5: PUPIL OWNED DEVICES

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. Pupils should only use the C2k Wi-Fi (C2K Wireless) when using their own device at school.

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.

Conditions for pupils using their own devices:

- The device must be used in accordance with the e-Safety and Acceptable Use of the Internet Policy;
- 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;

- Pupils should have an up-to-date anti-virus/Internet security product on their device;
- Acceptance that the school takes no responsibility for any device brought into school;
- Parents/Guardians should have appropriate insurance measures in place to cover the device for this application.
- 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;
- 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;
- If a teacher suspects school rules have been broken, pupils can be asked to display images stored on their device;
- If inappropriate and/or illegal materials are discovered, then the incident will be pursued through the schools' disciplinary procedure;
- 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;
- 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;
- Devices should be named ideally with a UV pen in accordance with advice from the police;
- 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;
- 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;
- Any charging device brought to school must be available for PAT testing to ensure electrical safe compliance;
- 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;
- 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.

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 into 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.

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).

SECTION 6: SAFETY RISK REGISTER

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.

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 (Appendix 4) will be completed.

SECTION 7: THE POLICY

Promoting of the 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.

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.

Approval steps in developing this policy.

This policy had originally been jointly developed alongside Strathearn, Grosvenor and Sullivan Upper schools. Revisions have 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.

Connections with other policies

The e-Safety and Acceptable Use of the Internet Policy operates in conjunction with other school policies including.

- Safeguarding and Child Protection Policy
- Positive Relationships and Anti-Bullying Policy.
- Social Media Policy
- Blended Learning Policy

SECTION 8: DATES OF POLICY REVIEW

Reviewing Committee: Education Committee

Review Date	Nature of Review	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
October 2020	Minor amendments	26 November 2020
May 2022	Amendments	23 June 2022
May 2024	Full Review	20 June 2024
February 2025	No amendments	27 February 2025
February 2026	Minor Amendments	26 February 2026

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 schoolwork. 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

This form is included in the Consent Section of the Data Collection Booklet completed by New Pupils

Bloomfield Collegiate Pupil Internet Access

and 'Bring Your Own Device' Consent Form

Please complete and return this form to enable your child to access the Internet at school. The form also authorizes your child 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 are confirming:

1. You have read and understood the e-Safety and Acceptable Use of the Internet Policy and agree to abide by this policy.
2. That a device brought to school by your child will **only be used in** accordance with this policy.
3. That you accept full responsibility for the full replacement value of all electronic equipment which the pupil mentioned below brings into school.
4. You 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. You 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 school's Disciplinary Policy.

This contract will remain in force **throughout your child'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 child 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), Pupil Owned Devices (Section 5) and Pupil Acceptable Use Agreement form (Appendix 6). I will use the computer system, including my own devices, in a responsible way and always obey the school rules.

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

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: _____

Authorised by: _____
(Vice Principal)

Date: _____

This form should be passed to the Vice Principal

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?

Staff (and Volunteer) Acceptable Use Agreement School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should always have an entitlement to safe access to the internet and digital technologies.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work. The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed E-Safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.

- I understand that the rules set out in this agreement also apply to use of these technologies (e.g., laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.

- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

- I will immediately report any illegal, inappropriate, or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language, and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in

accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Emails to parents should be directed through the info@ or school comms accounts. Any such communication will be professional in tone and manner. HOY/DT/SLT can use school email addresses when appropriate, (for example communicating with a pupil with long term absence).
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- All school Social Media accounts should be controlled with the staff members C2K address only and personal email addresses for such websites should not be used.

The school and the Education authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use.
- I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School.

Personal Data Policy.

- Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that GDPR policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that Bloomfield Collegiate School I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened. When using the internet in my professional capacity or for school sanctioned personal use:
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I will not allow pupils to use a computer or Device that I am logged into, this includes sending emails from teacher accounts.

- I understand that I am responsible for my actions in and out of the school:
- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Education Authority and in the event of illegal activities the involvement of the police. I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

I have read and understood the above policy.

Print name _____

Sign _____

Date _____

Pupil Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.
This Acceptable Use Agreement is intended to ensure that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use. that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.
For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger" when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I understand that everyone has equal rights to use technology as a resource and:
- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so. I will act as I expect others to act toward me:
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive, or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:
- I will only use my own personal devices (mobile phones / USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download, or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will immediately report any damage or faults involving equipment or software; however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I understand that I am responsible for my actions, both in and out of school:
- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Agreement; to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

- I have read and understand the above and agree to follow these guidelines when:
- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g., mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g., communicating with other members of the school, accessing school email, VLE, website etc.

Name of Pupil:
Class:
Signed:
Date:
Parent / Carer Countersignature:

Bloomfield Collegiate School
excellence in a caring community