Abbey Gate College

POLICY: Online Safety (incl. Pupil Acceptable Use)	
Scope	**Whole College**
Responsibility	**Deputy Head (Pastoral)**
Reviewed & Updated	**February 2025**
Governor Approval	**Vanessa Brodie**
Board Level Approval	**Andrew Grime**

CONTENT HYPERLINKS

Policy Statement (1)
Policy Statement (2)
Key Personnel

Roles and Responsibilities

Practice (1) – Education & Training
Practice (2) – Use of College & Personal Devices (incl. Mobile Phones)
Practice (3) – Use of Internet & Email

Practice (4) – Data Storage & Processing
Practice (5) – Password Security
Practice (6) – Safe Use of Digital & Video Images
Practice (7) – Misuse
Practice (8) – Complaints

APPENDIX 1: Bring Your Own Device (Pupils)
APPENDIX 2: Acceptable Use Code of Conduct (Pupils)
APPENDIX 3: Home/Remote Learning Responsible User Agreement

Policy Statement (1)

It is the duty of Abbey Gate College to ensure that every pupil in its care is as safe as reasonably possible; and the same principles apply to the digital world as apply to the real world. Information technology and online communications provide unrivalled opportunities for enhanced learning, in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are, therefore, taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of: identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of the College include:

- Websites;
- Email and instant messaging;
- Blogs;
- Social networking sites;
- Chat rooms;
- Music / video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles; and
- Mobile internet devices such as smart phones, tablets, and watches; and AI

This policy, supported by the *Acceptable Use* policies for all staff, visitors and pupils (ref. *Appendix 1 and 2*) is implemented to protect the interests and safety of the whole College community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements.

Both this policy and the *Acceptable Use* policy (for all staff, visitors and pupils) cover both fixed and mobile internet devices provided by the College (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto College premises (personal laptops, tablets, smart phones, etc.).

At Abbey Gate College we understand the responsibility to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about online safety, actively seeking their feedback, and listening to their fears and anxieties as well as their thoughts and ideas.

Policy Statement (2)

1) This policy applies to all members of the Abbey Gate College community, including:
    a. those in our EYFS setting;
    b. staff (including: teaching and non-teaching staff, governors, and regular volunteers);
    c. pupils;
    d. parents and visitors, who have access to and are users of the College IT systems ('Parents includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the College, including occasional volunteers).
2) Abbey Gate College implements this policy through adherence to the procedures set out in the rest of this document.
3) This policy is made available to all interested parties on the College website at www.abbeygatecollege.co.uk. It should be read in conjunction with the College's *Anti-Bullying, Behaviour, Code of Conduct, Data Protection, Health & Safety, PSHE (including Online Safety), and Safeguarding (including Child-on-Child Abuse)* policies.
4) Abbey Gate College is fully committed to ensuring that the application of this policy is non-discriminatory in line with the UK Equality Act (2010). Further details are available in the College's *EDI* policy document.
5) This policy is reviewed at least annually, or as events or legislation changes require, by the College Leadership Team and the Governing Body. The deadline for the next review is no later than 12 months after the most recent review date indicated above.
6) The most recent updates were made on account of an annual review.

Key Personnel

1) Craig Jenkinson: Head
2) Carole Houghton: Deputy Head (Pastoral) & DSL
3) Marie Hickey: Head of Infant & Junior School
4) Aaran Rose: IT Systems and Network Manager
5) Vanessa Brodie: Chair of Wellbeing Committee

Roles and Responsibilities

The Governing Body of the College is responsible for the approval of this policy and for reviewing its effectiveness.

The Head is responsible for the safety of the members of the College community and this includes responsibility for online safety. The Head has delegated day-to-day responsibility to the Designated Safeguarding Lead (Deputy Head (Pastoral)). In particular, the role of the Head and the Leadership Team is to ensure that:

- Staff (including Governors), in particular the Designated Safeguarding Lead are adequately trained about online safety; and

- staff are aware of the College procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the College.

The Designated Safeguarding Lead is the online safety co-ordinator. They are responsible to the Head for the day to day issues relating to online safety and for ensuring this policy is upheld by all members of the College community, working with ICT support staff to achieve this. They will keep up to date on current online safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board.

The IT Systems and Network Manager & IT Support Staff have a key role in maintaining a safe technical infrastructure at the College and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the College's hardware system, its data and for training the College's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the online safety coordinator/ designated safeguarding lead.

All Teaching and Support Staff are required to sign the *Acceptable Use* policy before accessing the College's systems. As with all issues of safety at this College, staff are encouraged to create a talking and listening culture in order to address any online safety issues which may arise in classrooms on a daily basis.

All Pupils are responsible for using the College IT systems in accordance with the *Acceptable Use* policy, and for letting staff know if they see IT systems being misused. Guidance with regard to online safety is included in pupils' annual planners.

Abbey Gate College also believes that it is essential for parents to be fully involved with promoting online safety both in and outside of College. We regularly consult and discuss online safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The College will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the College. Parents are made aware via the College's VLE what systems the College uses to filter and monitor online use, of what their children are being asked to do online, including the sites they will asked to access and are given clear guidance who (if anyone) their child is going to be interacting with online. Parents and carers are responsible for endorsing the College's Pupil *Acceptable Use* policy.

Practice (1) – Education & Training

Staff

1) New staff receive information on Abbey Gate College's online safety and *Acceptable Use* policies as part of their induction.
2) All teaching staff and governors receive regular information and training on online safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. All supply staff and contractors receive information about online safety as part of their safeguarding briefing on arrival at College.
3) All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following College online safety procedures. These behaviours are summarised in the *Acceptable Use* policy which must be signed and returned before use of technologies in College. When children use College computers, staff should make sure children are fully aware of the agreement they are making to follow the College's IT guidelines.
4) Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the College community.
5) The Designated Safeguarding Lead/Deputy Designated Safeguarding Lead must be notified, as soon as possible, about incidents relating to online safety.

Pupils

1) IT and online resources are used increasingly across the curriculum. We believe it is essential for online safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our pupils' understanding of it.
2) The College provides opportunities to teach about online safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside College will also be carried out via PSHE, by presentations in assemblies, as well as informally when opportunities arise.
3) At age-appropriate levels, and usually via PSHE, pupils are taught about their online safety responsibilities and to look after their own online safety. From Year 7, pupils are formally / informally taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the Designated Safeguarding Lead, and any member of staff at the College.
4) From year 7, pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities.
5) Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the College's *Anti-bullying*

policy, which describes the preventative measures and the procedures that will be followed when the College discovers cases of bullying). Pupils should approach the Designated Safeguarding Lead as well as parents, peers and other College staff for advice or help if they experience problems when using the internet and related technologies.

Parents

1) The College seeks to work closely with parents and guardians in promoting a culture of online safety. The College will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the College.
2) The College shares online resources and websites used by academic departments with parents via the College's VLE.
3) The College recognises that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home and provides information to develop their knowledge and understanding.

Practice (2) – Use of Mobile Phones

Pupils

1) For clarification, the College understands mobile phones to include SmartWatches or similar. The College accepts that pupils are permitted to bring such devices to College, but their use is restricted to the following guidelines; in order to promote an effective context of wellbeing and regulate pupils' online access, for safeguarding.
2) All mobile phones are brought into College at the pupils' own risk and the responsibility for their safekeeping lies with the pupil. The College will take no liability for loss or damage.
3) In the Infant & Junior School, pupils must hand their mobile phone in to Reception, where it will be kept in a locked unit and may be collected at the end of the school day.
4) College is a place of wellbeing and work; pupils' mobile phones must be switched off and be out of sight from 08.35 until 15.50 whilst on Senior School premises.
5) The exception to the above is that students in the Sixth Form; given their respective maturity and self-efficacy; are allowed to use their phones only in their Common Room. If they use their phones outside of the Sixth Form Common Room, they should expect the same intervention as the rest of the College, as below.
6) Permission must be sought from a member of staff, and authorisation given, before a pupil may be allowed to use a mobile phone on College premises.
7) If the usage of a mobile phone or similar is permitted or directed in a lesson (e.g. as a calculator, camera or voice recorder, depending on the subject) it will be under explicit staff supervision. However, every effort should be made to enable pupils to access digital resources through the VLE, including information slides and annotated screens.

8) Any pupil found using a mobile phone or similar on College premises without staff permission, should ordinarily expect to be reminded of College policy and for their mobile phone to be confiscated for the remainer of the College day. Repeated and apparently wilful lack of co-operation for any individual would result in an escalation of intervention and potential sanction.
9) If a pupil needs to contact home in an emergency, they must speak with a member of staff who will deal with the matter. Pupils should not contact home in the case of illness; this should only be done by a member of staff.
10) If parents need to contact pupils in an emergency, they should contact the College reception and a message will be taken to the pupil. Parents are reminded that pupils should not have their mobile phones turned on whilst on College premises and, hence, will be unable to check for messages.
11) The College recognises that mobile phones or similar are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile phone for such purposes, the pupil's parents or carers should request and make specific arrangements through, as appropriate, the Head, the Lead First-Aider, the Head of Learning Enrichment, or the Head of Year. Once practicalities have been agreed by all concerned, the relevant member of staff in each circumstance will then inform the pupil's teachers and other staff about how the pupil will use their phone at College.
12) Pupils may only access the internet through the College's network; no independent internet access is permitted.

Practice (3) – Use of Internet & Email

Pupils

1) All pupils are issued with their own personal College email addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all College work, assignments / research / projects. Pupils should be aware that email communications through the College network and College email addresses are monitored.
2) There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for College work / research purposes, pupils should contact the ICT department for assistance.
3) Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to the CLT pastoral lead in the school.
4) The College expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

5) Pupils must report any accidental access to materials of a violent or sexual nature directly to the pastoral lead in the school, or another member of Leadership. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the College's *Behaviour* policy. Pupils should be aware that all internet usage via the College's systems and its WiFi network is monitored.
6) Certain websites are automatically blocked by the College's filtering system. If this causes problems for College work / research purposes, pupils should contact ICT support department for assistance.
7) The College enables the use of pupil-owned tablets/devices as a teaching and learning tool and pupils are required to adhere to the *Pupil BYOD* policy (Appendix 2) when using tablets for College work. In particular, the *BYOD* policy requires pupils to ensure that their use of tablets/devices for College work complies with this policy and the *Acceptable Use* policy and prohibits pupils from using tablets/devices for non-College related activities during the College day.
8) Pupils should be aware that under no circumstances should they enter an examination venue with an unauthorised device, even if it is switched off. To do so will lead to disqualification from that examination and potentially other examinations.
9) Pupils should note that the use of all and any devices on College premises is subject to the College's *Acceptable Usage* policy.

Practice (4) – Data Storage & Processing

1) The College takes its compliance with the Data Protection Act 1998 seriously. Please refer to the *Privacy* notices and *Data Protection Handbook* for further details.
2) Staff and pupils are expected to save all data relating to their work to their College laptop/ PC or to their Microsoft One drive.

Practice (5) – Password Security

Pupils and staff have individual College network logins and email addresses. Staff and pupils are regularly reminded of the need for password security. All pupils and members of staff should:

- use a strong password (usually containing six characters or more, and containing upper and lower case letters as well as numbers), which should be changed every 30 days.
- not write passwords down; and
- not share passwords with other pupils or staff.

Practice (6) – Safe Use of Digital & Video Images

1) The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital

images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

2) Of more recent concern is the increase in the use of AI to manipulate innocent images into indecent images or videos. The 2024 report from the IWF, which details the increasing scale of this can be found here.
3) When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).
4) Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy and related, concerning the sharing, distribution and publication of those images. Those images should only be taken on College equipment: personal equipment should not be used for such purposes.
5) Care should be taken when taking digital / video images for potential posting on social media, website, or other digital publications that they:

- DO NOT show an individual child's face in full, frontal profile (such as may easily be cut and pasted elsewhere)
- DO show children from behind, in groupings, in side profile, or partially obscured (such that any individual cut/paste would be notably difficult)
- DO consider potential safeguarding implications, before taking the shot (for example, young people in tracksuits or similar, rather than revealing kit - for both male and female)

6) Images must not show pupils participating in activities that might bring the individuals or the College into disrepute.
7) Pupils must not take, use, share, publish or distribute images of others.
8) Written permission from parents or carers will be obtained before photographs of students / pupils are published on the College website (see Parent Contract / *Acceptable Use* policy for more information).
9) Photographs published on the College website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with ISA guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Practice (7) – Misuse

1) Abbey Gate College will not tolerate illegal activities or activities that are inappropriate in a College context, and will report illegal activity to the police and/or the LSCB. If the College discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the CEOP.
2) Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the College's policies and procedures (in particular the *Safeguarding* policy).

3) The College will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our *Anti-Bullying* policy.

Practice (8) – Complaints

As with all issues of safety at Abbey Gate College, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to online safety prompt action will be taken to deal with it. Please see the *Complaints* policy for further information.

APPENDIX 1: Bring Your Own Device (Pupils)

The College recognises that mobile technology offers valuable benefits to pupils from a teaching and learning perspective. Our College embraces this technology but requires that it is used in an acceptable and responsible way.

This policy is intended to address the use by pupils of non-College owned electronic devices to access the internet via the College's internet connection, to access or store college information, or to make photographs, video, or audio recordings at the College. These devices include tablets, laptops, and any similar devices. If you are unsure whether your device is captured by this policy please check with the College's ICT support department.

This policy is supported by the Pupils' Acceptable Use Code of Conduct.

Policy Statements

1. Use of laptops/tablets at the College

Pupils may use their own laptops/tablets in the following locations:

- In the classroom with the permission of the teacher
- In the College common areas for example library, common rooms. (Senior School only)

Pupils are responsible for their laptop/tablet at all times. The College is not responsible for the loss or theft of or damage to the laptop/tablet or storage media on the device (e.g. removable memory card) howsoever caused.

Laptops/tablets must be turned off when in a prohibited area and/or at a prohibited time and must not be taken into controlled assessments and/or examinations, unless special circumstances apply. Please refer to the College Examinations Officer for examination guidance.

The College reserves the right to refuse pupils permission to use their own laptops/tablets on College premises.

2. Use of cameras and audio recording equipment

Pupils should **not** use their own laptops/tablets to take photographs, video, or audio recordings in College without obtaining permission. This includes people who might be identifiable in the background.

To respect everyone's privacy and in some cases protection, photographs, video, or audio recordings should not be published on blogs, social networking sites or in any other way without the permission of the people identifiable in them.

No one must use laptops/tablets to record people at times when they do not expect to be recorded, and devices must not be used that would enable a third party acting remotely

to take photographs, video, or audio recordings in College. Pupils must comply with the College's Behaviour Policy, and Anti-Bullying policy when making photographs, videos, or audio recordings.

3. Access to the College's internet connection

The College provides a wireless network that pupils must use, to connect their laptop/tablet to the internet. Access to the wireless network is at the discretion of the College, and the College may withdraw access from anyone it considers is using the network inappropriately.

The College is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto the user's own device whilst using the College's wireless network. This activity is taken at the owner's own risk and is discouraged by the College. The College will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the College's wireless network.

4. Access to College IT services

Pupils are permitted to connect to or access the following College IT services from their laptop/tablet:

- the College virtual learning environment.
- the internet.

Pupils must only access these services using their mobile devices via the College's secure segregated Wi-Fi.

If in any doubt a device user should seek clarification and permission from the College's ICT support team before attempting to gain access to a system for the first time. Users must follow the written procedures for connecting to the College systems.

5. Monitoring the use of laptops/tablets or similar

The College may use technology that detects and monitors the use of mobile and other electronic or communication devices which are connected to or logged on to our wireless network or IT systems. By using a mobile device on the College's IT network, pupils at the college agree to such detection and monitoring. The College's use of such technology is for the purpose of ensuring the security of its IT systems, tracking College information.

6. Security of pupils' laptops/tablets

Pupils must take all sensible measures to prevent unauthorised access to their laptops/tablets, including but not limited to the use of a PIN, pattern or password to be entered to unlock the device, and ensuring that the device auto-locks if inactive for a period of time.

Pupils must never attempt to bypass any security controls in College systems or others' own devices.

Pupils are reminded to familiarise themselves with the College's Online Safety procedures (which includes social media and acceptable use of IT policies which set out in further detail the measures needed to ensure responsible behaviour online.)

Pupils must ensure that appropriate security software is installed on their laptops/tablets and must keep the software and security settings up-to-date.

7. Compliance with Data Protection Policy

Pupils compliance with this BYOD policy is an important part of the College's compliance with the Data Protection Act 1998. Pupils must apply this BYOD policy consistently with the College's Data Protection Policy.

8. Support

The College ICT Support department will help to support pupils accessing College approved systems; however, the College takes no responsibility for supporting pupil's own devices; nor has the College a responsibility for conducting annual PAT testing of personally-owned devices.

9. Compliance, Sanctions and Disciplinary Matters

Non-compliance of this policy exposes both pupils, staff and the College to risks. If a breach of this policy occurs the College will respond immediately in accordance with behavioural policy. Guidance will also be offered. If steps are not taken by the individual to rectify the situation and adhere to the policy, then the mobile device in question may be confiscated and/or permission to use the device on college premises will be temporarily withdrawn. For persistent breach of this policy, the College will permanently withdraw permission to use user-owned devices in the College.

10. Incidents and Response

Loss or theft of the mobile device should be reported to Reception in the first instance. The College is not responsible for any losses or damages to personal devices. It is highly recommended that pupils/parents/staff take precautionary insurance to cover any such circumstances, this is not the responsibility of the College.

11. Request for parental consent

Any individual images of potential concern to us, we will seek your specific consent for us to use/post the image. Informed consent from your perspective would include awareness and understanding of data protection as well as safeguarding, where any online image with unrestricted, public access is then beyond the College's control and may be subject to malicious mis-use.

12. Instructions for all parental events.

For reasons of data protection and safeguarding, photographs of any young people in this event, on personal devices and cameras, is not permitted. If photography of own children is allowed, in a specific context with College instruction, and includes other

children alongside or in the background, it must not be uploaded to any public, unprotected digital domain without the prior, written consent of each family involved. The College also makes parents aware that any online image with unrestricted, public access is beyond the College's or any parent's control, and may be subject to malicious mis-use.

APPENDIX 2: Acceptable Use Code of Conduct (Pupils)

Abbey Gate College pupils are required to accept these rules as a condition of logging on to school facilities. They apply to all uses, whether on or off-site; using networked or mobile computers; school or personal devices; tablets or smart phones.

All our pupils should act with consideration, common sense and good manners at all times. Any violation of this policy should be reported to a teacher immediately.

User Accounts

- ☐ Pupils must keep their password secret.
- ☐ Pupils must never use a computer whilst logged on as another person.
- ☐ Pupils must observe copyright restrictions (e.g. on material from CD-ROMs or the internet).

Computer Equipment

- ☐ Unsupervised pupils may not use computers or smartboards in classrooms or laboratories without permission.
- ☐ Pupils must not damage, disable or otherwise harm the operation of computers.
- ☐ Pupils must not eat or drink near computer equipment.

Offensive Material

Pupils must not use ICT to view, send or store offensive material.

Hacking

Hacking is illegal and is forbidden. This includes attempting to gain access to any file, function or network area which a pupil does not have permission to view or use. Pupils must not attempt to bypass monitoring software.

Rogue Files

Pupils must not at any time have software on the network (e.g. files ending in .EXE, .COM or files containing these). If pupils use compressed files (e.g. those ending in .ZIP) they must un-compress them before logging off.

Pupils must not use the network to store files which are solely for their personal recreation or files which cannot be accessed using software available at school.

E-mail

- ☐ Pupils must not use internet-based e-mail services (such as Hotmail) other than the filtered Abbey Gate College system.
- ☐ Pupils may not send e-mails which appear to be either anonymous or from another person.
- ☐ Pupils may not send bulk e-mails (i.e. e-mails to more than five recipients) unless a teacher gives prior consent.
- ☐ Pupils may not copy or forward e-mails without permission

VLE (Firefly)/Microsoft Teams

When using the VLE/MSTeam's communication facilities, pupils must:

- ☐ Respect other people's views and beliefs
- ☐ Only post items which are appropriate

When using the VLE's communication facilities, pupils must NOT:

- ☐ Behave in an impolite or offensive manner.
- ☐ Post anything abusive, defamatory, obscene or otherwise illegal
- ☐ Post any personal or private information on any individual
- ☐ Post material which contains viruses or other programs which may disrupt the school systems

Copyright

Copyright of the study material and all other content of the VLE is owned or controlled by Abbey Gate College. Pupils are permitted to view, copy and print documents within the VLE subject to their agreement that:

- ☐ Use of the material is for pupil's own personal information, and for non-commercial purposes only
- ☐ Pupils will not modify the documents or graphics in any form or manner
- ☐ Pupils will not copy or distribute graphics separately from their accompanying text and will not quote materials out of their context.

When submitting postings or assignments within the VLE, pupils must give due acknowledgement for material quoted from other sources, both within the VLE and elsewhere.

Internet

The internet may only be used for research related to academic subjects, Higher Education or Careers, i.e. for educationally beneficial tasks rather than recreational use such as games. Pupils may not use 'chat' services. Online purchasing of goods or services is not allowed.

Monitoring

Pupils should be aware that any use of the school network is monitored to ensure appropriate usage. This includes the remote scanning of computer monitors, the checking of files and e-mails, and the analysis of internet sites visited.

Prevent Duty

Filtering systems, including 'Policy Central' which has a module for the application of the Prevent Duty, are in place to prevent individuals from accessing extremist websites at Abbey Gate College, and therefore ensuring all pupils and staff are safe from terrorist and extremist material when using the internet in school.

However, in the eventuality of any individual accessing material which could result in them being drawn into terrorism they will be referred to the Single Point of Contact (SPOC) who will then follow the Prevent Duty protocol in the Safeguarding Policy.

Printing

- ☐ Pupils must take care not to print excessive amounts, nor to waste paper
- ☐ Pupils must obtain a teacher's permission before printing

Cyber Bullying

Pupil use of social networking sites should not be hurtful to pupils or staff, here or elsewhere, neither should it bring the School's name into disrepute. Cyber bullying - deliberately hurtful behaviour either over the internet or with mobile phones - is addressed in PSHE lessons and in regular workshops for pupils and parents and is dealt with in the same manner as all bullying and child-on-child abuse.

Games

Pupils are not allowed to email or bring recreational games to play at school, unless this has been authorised by a teacher.

Taking, Storing and Publishing Photographs and Recordings

No pupil or anyone else should be taking or storing pictures or sound recordings on Abbey Gate College premises without good reason and the appropriate prior permissions, both of the College and of anyone appearing in the images/recordings.

Similarly, pupils are not allowed to publish web pages, photographs or recordings of pupils, staff or school premises, without permission of the College.

Mobile Phones

- ☐ Pupils may bring their phone to College but should not use this between the start and end of the school day, unless they have been given permission by a member of staff.
- ☐ Pupils at the Infant and Junior School must switch off phones on arrival and hand them in at reception.
- ☐ Pupils must not play music through speakers.
- ☐ Pupils must not take any photographs or video.
- ☐ Pupils must not use their phones whilst walking along the corridors at any time of the day.

- ☐ Phones must be switched off during lessons unless the teacher has given permission.
- ☐ If a pupil is ill they MUST see the Lead First-Aider who will contact home if appropriate.

Sanctions

If any pupil violates the provisions of this policy, action will be taken by the College in line with existing policy regarding behaviour. This could include serious sanctions and, where appropriate, other authorities.