Archbishop Beck Catholic College

Acceptable User Policy
Staff, Governors and Volunteers

What is an Acceptable User Policy (AUP)?

We ask all children, young people and adults involved in the life of Archbishop Beck Catholic College to sign an Acceptable User Policy (AUP), which outlines how we expect them to behave when they are online, and / or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school). This AUP is reviewed annually,

Why do we need an AUP?

All staff (including support staff), governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy. The full 'Online Safety Policy' for Archbishop Beck Catholic College is available on the college website.

Where can I find out more?

All staff, governors and volunteers should read Archbishop Beck Catholic College's full Online Safety Policy that is available on the college website for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc).

If you have any questions about this AUP or our approach to online safety, please speak to a member of the safeguarding team who can contacted at info@beck.uk.com or contact the main office on 0151 525 6326.

What am I agreeing to?

1. Staff and governors): I have read and understood Archbishop Beck Catholic College's full Online Safety policy that is available in full on the college website and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
2. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (Miss Emma Griffiths (if by a child) or Headteacher Mr Paul Stirling (if by an adult).
3. I understand the responsibilities listed for my role in the school's Online Safety policy. This includes promoting online safety as part of a whole school approach in line with safeguarding considerations when supporting pupils remotely.
4. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured / viewed by the relevant authorised staff members.
5. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, e.g. by:
   - not sharing other's images or details without permission
   - refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
6. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames / handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach

of this by others or attempts by pupils to do the same to the Headteacher and safeguarding lead.

7. Details on social media behaviour, the general capture of digital images / video and on my use of personal devices is stated in the full Online Safety policy. If I am not sure if I am allowed to do something in or related to school, I will not do it before taking advice.

8. I understand the importance of upholding my online reputation, my professional reputation and that of the school, and I will do nothing to impair either. More guidance on this point can be found in this [Online Reputation](#) guidance for schools and in Archbishop Beck Catholic College's social media policy/guidance.

9. I agree to adhere to all provisions of the school Data Protection Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords / logins and other access, never share credentials and immediately change passwords and notify Mr David Cummins or Mrs Dawn Bond if I suspect a breach. I will only use complex passwords and not use the same password as for other systems.

10. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature by the school.

11. I understand and support the commitments made by pupils / students, parents and fellow staff, governors and volunteers in their Acceptable Use Policies available in full on the college website and will report any infringements in line with school procedures.

12. I understand that breach of this AUP and / or of the school's full Online Safety Policy available in full on the college website may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authority.

To be completed by the user

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____

Name: _____

Role: _____

Date: _____

To be completed by <mark>**[insert here the name/s and role/s of the member of staff with delegated authority from the Headteacher/Principal to issue access/usage permissions]**</mark>

I approve this user to be allocated credentials for school systems as relevant to their role.

Systems: _____

<mark>**[ask your network manager to give you a list of systems or categories to insert here]**</mark>

Additional permissions (e.g. admin): _____

Signature: _____

Name: _____

Role: _____

Date: _____