ASKHAM BRYAN COLLEGE

Privacy and Electronic Communications Regulations Policy 2026 - 2028

Equality Impact Assessment: Askham Bryan College recognises the importance of the Equality Act 2010 and its duties under the Act. This document has been assessed to ensure that it does not adversely affect staff, students or stakeholders on the grounds of any protected characteristics.

1. POLICY STATEMENT

1.1 The Privacy and Electronic Communications Regulations ("PECR") sit alongside the Data Protection Act 2018 and the UK GDPR. They are derived from European law. The PECR implement European Directive 2002/58/EC, also known as "the e-privacy Directive". They give people specific privacy rights in relation to electronic communications[1].

1.2 There are specific rules on:

- direct marketing, using marketing calls, emails, texts and faxes or any other type of 'electronic mail' (picture messages, video messages, voicemails, direct messages via social media or any similar message that is stored electronically);
- cookies (and similar technologies);
- keeping communications services secure; and
- customer privacy as regards traffic and location data, itemised billing, line identification (e.g. caller ID and call return), and directory listings.

1.3 The PECR have been amended a number of times. The latest version came into effect on 29th March 2019.

1.4 Only the rules on direct marketing and cookies, however, are likely to apply to the College. A lot of the rules only apply if you are a network or service provider[2].

1.5 Where the College is involved in marketing by electronic means to individuals or uses cookies or similar technologies, it will ensure that at all times, it complies with the PECR in addition to the UK GDPR and the Data Protection Act 2018.

[1] "Electronic communications" mean any information sent between particular parties over a phone line or internet connection. This includes phone calls, faxes, text messages, video messages, emails and internet messaging. It does not include generally available information such as the content of web pages or broadcast programming.

[2] A "service provider" provides telephone or internet services; a "network provider" provides the underlying network equipment.

2. SCOPE AND LIMITATIONS

2.1 This Policy applies across all sites; to any staff sending unsolicited marketing messages.

3. DIRECT MARKETING

3.1 "Direct marketing" is defined in section 122(5) of the Data Protection Act 2018 as "the communication (by whatever means) of advertising or marketing material which is directed to particular individuals". This covers all advertising or promotional material, including that promoting the aims or ideals of not-for-profit organisations – for example, it covers a charity or political party campaigning for support or funds.

3.2 Most of the rules in the PECR only apply to unsolicited marketing messages. They do not restrict solicited marketing.

Solicited vs unsolicited marketing

3.3 A solicited message is one that is actively requested.

3.4 An unsolicited message is any message that has not been specifically requested.

3.5 You can still send unsolicited marketing messages – as long as you comply with the PECR. Often this means you will need someone's consent to send them an unsolicited marketing message; but there are exceptions.

Routine customer service messages

3.6 Routine customer service messages do not count as direct marketing – in other words, correspondence with customers to provide information they need about a current contract or past purchase (e.g. information about service interruptions, delivery arrangements, product safety, changes to terms and conditions, or tariffs). General branding, logos or straplines in these messages do not count as marketing.

Mailshots

3.7 The PECR marketing provisions also do not apply to other types of marketing, such as mailshots or online advertising.

Significant promotional material

3.8 However, if the message includes any significant promotional material aimed at getting customers to buy extra products or services or to renew contracts that are coming to an end, that message includes marketing material and the rules apply.

4. SOFT OPT IN

What is a 'soft opt-in'?

4.1 The term 'soft opt-in' is sometimes used to describe the rule about existing customers. The idea is that if an individual bought something from a business recently, gave that business their details, and did not opt out of marketing messages, they are probably happy to receive marketing from the business about similar products or services even if they have not specifically consented. However, they must have been given a clear chance to opt out – both when the business first collected their details, and in every message sent after that.

4.2 The soft opt-in rule means the College may be able to email or text people who have contacted the College and expressed an interest in coming to the College provided the above conditions are satisfied.

5. CONSENT

5.1 To ensure the College complies with its obligations under the PECR, the College will ensure that it has an individual's consent for any direct marketing.

5.2 The PECR uses the UK GDPR standard of consent, i.e. to be valid, consent must be knowingly and freely given, clear and specific.

5.3 "Freely given" means giving people genuine ongoing choice and control over how the College uses their data. The individual must also fully understand that they are giving consent and what this is for.

5.4 An individual also has the right to withdraw their consent at any time.

5.5 The clearest way to obtain consent is to ask the individual to tick an unticked opt-in box confirming they are happy to receive marketing calls, faxes, texts or emails.

6. EXEMPTIONS

6.1 There are a limited number of exemptions from the PECR:

a) a national security exemption
b) a law and crime exemption
c) the cookies exemptions.

The national security exemption

6.2 The national security exemption is in Regulation 28 PECR. It exempts communications providers from any of the rules in PECR if the communication provider reasonably needs to breach that Regulation for the purpose of safeguarding national security.

6.3 A Minister of the Crown can issue a certificate stating that an exemption was, is or will be required in certain circumstances for national security reasons. A ministerial

certificate is conclusive proof that the exemption applies in those circumstances. Any person directly affected by a ministerial certificate may appeal against it to the Information Rights Tribunal.

The law and crime exemption

6.4 The law and crime exemption is in Regulation 29. It exempts communications providers from any of the rules in PECR if complying with that rule would:

- breach a provision of another enactment;
- breach a court order;
- be likely to prejudice the prevention or detection of crime; or
- be likely to prejudice the apprehension or prosecution of offenders.

6.5 It also applies if the exemption is required (i.e., you need to breach that Regulation):

- for or in connection with any legal proceedings;
- to obtain legal advice; or
- to establish, exercise or defend legal rights.

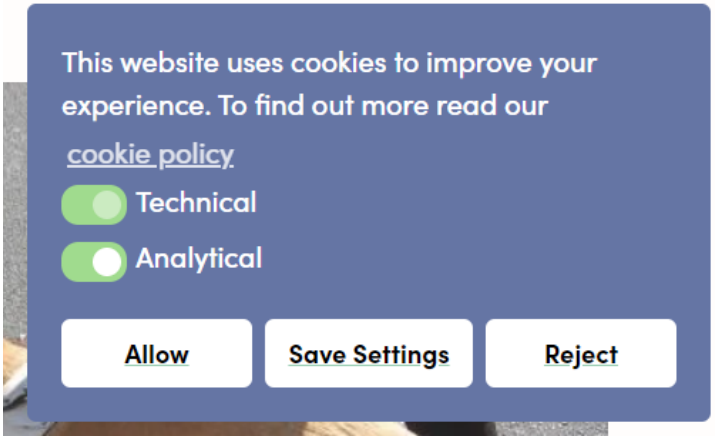
Cookies exemptions

6.6 A “cookie” is a small text file that is downloaded onto a computer or smartphone, etc when the user accesses a website. It allows the website to recognise that user’s device when it comes to use the website again and store some information about the user’s preferences or past actions.

6.7 The rules on cookies are in Regulation 6. The basic rule is that you must:

- tell people the cookies are there;
- explain what the cookies are doing and why; and
- get the person’s consent to store a cookie on their device.

6.8 Users accessing the College website will be told that the website uses cookies and will be asked to confirm their cookie preferences.



6.9 There is also a link to the Cookie Policy (https://www.askham-bryan.ac.uk/cookies-policy/).

6.10 There are two exemptions which apply where:

- the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or

- the cookie is strictly necessary to provide an 'information society service' (e.g. a service over the internet) requested by the subscriber or user. Note that it must be essential to fulfil their request – cookies that are helpful or convenient but not essential, or that are only essential for your own purposes, will still require consent.

6.11 This means the College is unlikely to need consent for:

- cookies used to remember the goods a user wishes to buy when they add goods to their online basket or proceed to the checkout on an internet shopping website;
- session cookies providing security that is essential to comply with data protection security requirements for an online service the user has requested – e.g. online banking services; or
- load-balancing cookies that ensure the content of your page loads quickly and effectively by distributing the workload across several computers.

7. COMPLAINTS

7.1 If you feel that the College has failed to comply with the PECR, then in the first instance, you should raise the matter with the College's Data Protection Officer by contacting judith.clapham@askham-bryan.ac.uk or by emailing DataProtection@askham-bryan.ac.uk or by contacting the Legal and Compliance Adviser at jethro.powell@askham-bryan.ac.uk .

7.2 In accordance with the College's Complaints Policy, all complaints will be acknowledged within 2 working days, and the College will endeavour to provide a response within 10 working days. If more time is needed to investigate your complaint and provide a response, we will let you know. If you are not satisfied with the College's response to your complaint, you have the right to appeal, and ultimately, the right to complain to the ICO.

7.3 If you make a complaint to the College's Data Protection Officer and are not satisfied with the College's response, then you may then wish to contact the Information Commissioner's Office (or "ICO"), the UK's supervisory authority and make a formal complaint (https://ico.org.uk/make-a-complaint/). Please note: although you may complain to the ICO at any time, the ICO is likely to ask you to exhaust the College's complaints process first, before it processes your complaint.

7.4 The College is registered with the Information Commissioner's Office ("ICO"). The Registration Number is Z6170811. Renewal of the registration takes place annually on 22 January.

8. RESPONSIBILITIES

8.1 The Head of Marketing will have overall responsibility for ensuring compliance with this policy.

8.2 The Head of Marketing and the Marketing team will have day-to-day responsibility for ensuring compliance with this policy.

9. MONITORING AND REVIEW

9.1 The Deputy Chief Executive Officer will maintain oversight of the effectiveness of these arrangements, assisted by the Legal and Compliance Adviser.

9.2 This policy and the implementation arrangements which underpin it will be reviewed annually by the Director of Governance and Legal and Compliance Adviser.

10. SUPPORTING/RELATED DOCUMENTS

Data Protection Policy
Subject Access Request Policy
Subject Access Request Procedure (internal use only)
Data Sharing Policy
Data Sharing Procedure (internal use only)
Data Retention Policy
Data Retention Procedure (internal use only)
Data Breach Reporting Procedure (internal use only)
Data Subject Rights Procedure (internal use only)

11. RELEVANT LEGISLATION

11.1 In all aspects of this policy the College will comply with the following legislation:

Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)
UK GDPR
Data Protection Act 2018

12. DOCUMENT HISTORY

Date of Issue: 2nd September 2026
Approved on: 15th July 2026
Next review: June 2028
Owner: Deputy Chief Executive Officer
Author: Legal and Compliance Adviser
Publication requirements: PUBLIC