CHELTENHAM
LADIES' COLLEGE

Online Safety Policy

2026-27

CHELTENHAM LADIES' COLLEGE

ONLINE SAFETY POLICY

Contents

AIMS 2
SCOPE AND APPLICATION 2
REGULATORY FRAMEWORK 2
PUBLICATION AND AVAILABILITY 4
DEFINITIONS 4
RESPONSIBILITY STATEMENT AND ALLOCATION OF TASKS 4
ROLE OF STAFF AND PARENTS 5
FILTERING AND MONITORING STANDARDS 8
DIGITAL AND SECURITY STANDARDS 9
ACCESS TO COLLEGE TECHNOLOGY 9
PROCEDURES FOR DEALING WITH INCIDENTS OF MISUSE 11
EDUCATION 12
TRAINING 13
RISK ASSESSMENT 15
RECORD KEEPING 16

1. AIMS

This is the online safety policy of Cheltenham Ladies' College (**College**).

The aim of this policy is to promote and safeguard the welfare of all pupils through the implementation of an effective online safety strategy which:

- protects the whole College community from illegal, inappropriate and harmful content or contact;
- educates the whole College community about their access to and use of technology; and
- establishes effective mechanisms to identify, intervene and escalate incidents where appropriate.
- Responds to pupil and staff feedback to ensure an effective and current online safety policy.
- creates a culture of safety, equality and protection.

2. SCOPE AND APPLICATION

This policy applies to the whole College.

This policy applies to all members of the College community, including staff and volunteers, pupils, parents and visitors, who have access to College technology whether on or off College premises, or otherwise use technology in a way which affects the welfare of other pupils or any member of the College community or where the culture or reputation of the College is put at risk.

3. REGULATORY FRAMEWORK

This policy has been prepared to meet the College's responsibilities under:

- Education (Independent School Standards) Regulations 2014;
- *Boarding schools: national minimum standards* (Department for Education (**DfE**), May 2026); Education and Skills Act 2008;
- Children Act 1989;
- Childcare Act 2006;
- Data Protection Act 2018, the UK General Data Protection Regulation (**GDPR**) and the Data (Use and Access) Act 2025 (collectively referred to as data protection laws);
- Equality Act 2010; and
- Charities Act 2011

This policy has regard to the following guidance and advice:

- Keeping children safe in education (KCSIE 2026)
- Preventing and tackling bullying (DfE, July 2017);

- Behaviour in Schools Advice for Headteachers and Staff 2024;
- Meeting Digital and Technology Standards in Schools and Colleges;
- Sharing nudes and semi-nudes: advice for educational settings December 2024
- Prevent_Duty_Guidance_for_England_and_Wales (HM Government, updated April 2023);
- Channel duty guidance 2023: Channel duty guidance: protecting people susceptible to radicalisation (accessible) - GOV.UK (www.gov.uk)
- Relationships education, relationships and sex education and health education guidance (DfE, June 2021) https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education Searching, screening and confiscation: advice for schools July 2022 ; Searching, Screening and Confiscation (publishing.service.gov.uk) and
- Childnet International Guidance for schools at Childnet Guidance for Schools.
- Sharing nudes and semi-nudes: advice for educational settings December 2024
- Generative AI
- Online safety in schools and colleges: questions from the governing board (UKCCIS, 2016)
- DfE Filtering and Monitoring Standards for Schools and Colleges updated June 2026 - Meeting Digital and Technology standards in Schools
- Cyber Security Standards for Schools and Colleges - Meeting Digital and Technology Standards in Schools
- Technology, planning and cyber security - Meeting the Cybersecurity Standards
- https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges
- Online – misinformation, disinformation and conspiracy theories - Pears Foundation
- Educate against Hate
- Countering Conspiracy theories

The following College policies, procedures and resource materials are relevant to this policy:

- ICT Acceptable Use Policy for Pupils;
- Staff ICT Acceptable Use Policy and Social Media Policy;
- Safeguarding (Child Protection) Policy;
- Anti-bullying and cyberbullying policy;
- Risk Assessment Policy for Pupil Welfare;
- Staff Code of Conduct and Whistleblowing Policy;
- Data Protection Policy for staff;
- Information Security Policy (including remote working and bring your own device to work);
- College rules; and
- Relationships Education, Relationships and Sex Education Policy.
- Mental Health Policy
- Search and Confiscation Policy

- Relationships Between Adults and Pupils Guidelines
- Pupil Relationships Policy
- Visitors Policy

4. PUBLICATION AND AVAILABILITY

This policy is published on the College website.

This policy is available on the Parent Portal.

This policy can be made available in large print or other accessible format if required.

5. DEFINITIONS

Where the following words or phrases are used in this policy:

- References to the **Proprietor** are references to Council.
- In considering the scope of the College online safety strategy, College will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information (collectively referred to in this policy as **technology**).

6. RESPONSIBILITY STATEMENT AND ALLOCATION OF TASKS

Council has overall responsibility for all matters which are the subject of this policy.

Council is required to ensure that all those with leadership and management responsibilities at College actively promote the well-being of pupils. The adoption of this policy is part of Council's response to this duty.

To ensure the efficient discharge of its responsibilities under this policy, Council has allocated the following tasks:

Task	**Allocated to**	**When / frequency of review**
Keeping the policy up to date and compliant with the law and best practice	DSL	As required, and at least termly
Monitoring the implementation of the policy (including the record of incidents involving the use of technology and the logs of internet activity and sites visited), relevant risk assessments and any action taken in response and evaluating effectiveness	DSL	As required, and at least termly
Online Safety	DSL	
Maintaining up to date records of all information created in relation to the policy and its implementation as required by the GDPR	Head of Digital Services	As required, and at least termly
Seeking input from interested groups (such as pupils, staff, Parents) to consider improvements to College processes under the policy	DSL	As required, and at least annually
Formal annual review	DSL	Annually

7. ROLE OF STAFF AND PARENTS

Executive Principal and Senior Leadership Team

The Executive Principal has overall executive responsibility for the safety and welfare of members of the College community.

The Designated Safeguarding Lead (DSL) is the senior member of staff from the College leadership team with lead responsibility for safeguarding and child protection, including online safety. The responsibility of the Designated Safeguarding Lead includes managing safeguarding incidents involving the use of technology in the same way as other safeguarding matters, in accordance with the College Child Protection and Safeguarding Policy and procedures.

The Designated Safeguarding Lead will work with the Head of Digital Services (see below) in monitoring technology uses and practices across College and assessing whether any improvements can be made to ensure the online safety and well-being of pupils. The Designated Safeguarding Lead will regularly monitor the technology incident logs maintained by the Head of Digital Services.

The Designated Safeguarding Lead is responsible for ensuring that staff are suitably trained in online safety to a level that is suitable to their particular role in College. The DSL will also regularly update other members of the College Senior Leadership Team on the operation of College safeguarding arrangements, including online safety practices.

The Head of Digital Services, together with his team, is responsible for the effective operation of the College filtering system so that pupils and staff are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the College network (currently WatchGuard)

The Head of Digital Services is responsible for ensuring that:

- College technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack;
- Users may only use College technology if they are properly authenticated and authorised;
- College has an effective filtering policy in place and that it is applied and updated on a regular basis;
- The risks of pupils and staff circumventing the safeguards put in place by College are minimised;
- The use of College technology is regularly monitored to ensure compliance with this policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation; and
- Monitoring software and systems are kept up to date to allow the ICT team to monitor the use of email and the internet over the College network and maintain logs of such usage.
- A firewall is used to filter, report on and manage internet connections. All connections to the Internet go through this firewall unless there is a technical reason, agreed by the Head of Digital Services, for them not to.
- The Head of Digital Services will report regularly to the ICT Steering group and on request to the Leadership Team on the operation of College technology. If the Head of Digital Services has concerns about the functionality, effectiveness, suitability or use of technology within College, including of the monitoring and filtering systems in place, they will escalate

those concerns promptly to the Designated Safeguarding Lead. The Designated Safeguarding Lead is responsible for maintaining the incident log of any matters of safeguarding concern brought to the attention of the Designated Safeguarding Lead in accordance with College Child Protection and Safeguarding Policy and procedures. The DSL will use CPOMS for these logs.

All Staff

All staff have a responsibility to act as good role models in their use of technology and to share their knowledge of College policies and of safe practice with the pupils.

All staff will receive appropriate online safety training as part of their safeguarding training at induction which will include an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

Staff are expected to adhere, so far as applicable, to each of the policies referenced in this policy.

Staff have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this policy and College child protection and safeguarding policy and procedures.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- **content**: being exposed to illegal, inappropriate, or harmful content, for example:

  pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories,

- **contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

- **conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, including those generated using AI and online bullying, and

- **commerce**: - risks such as online gambling, inappropriate advertising, phishing and or financial scams. Concerns that pupils or staff are at

risk, should be reported to the Anti-Phishing Working Group (https://apwg.org/).and discussed with the DSL and or Head of Digital Services.

In particular, staff should be mindful that the following areas are becoming increasingly prominent safeguarding concerns:

- Generative AI
- Deepfakes
- Financial exploitation via online platforms
- Online coercion and sextortion
- Algorithmic radicalisation
- Misinformation
- Disinformation
- Conspiracy Theories

Parents

The role of parents in ensuring that pupils understand how to stay safe when using technology is crucial. College expects parents to promote safe practice when using technology and to:

- support College in the implementation of this policy and report any concerns in line with College policies and procedures;
- talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour; and
- encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support.

If parents have any concerns or require any information about online safety, they should contact the Miss Caroline Ralph, Designated Safeguarding Lead. You may email any concerns to ralphcj@cheltladiescollege.org.

8. FILTERING AND MONITORING STANDARDS

College meets the filtering and monitoring standards as set out by the DofE and referenced in KCSIE. The Head of Digital Services is responsible for Filtering and monitoring which is aligned with the DfE's **Filtering and monitoring: core standard**. Part of these standards require us to keep records of filter and alerting checks, reports on usage, etc. Therefore, as outlined in this policy, College:

- Has assigned roles and responsibilities to manage filtering and monitoring systems.
- Reviews filtering and monitoring provision at least annually by the DSL, supported by the Head of Digital Services and with NCMS oversight.

- Blocks harmful and inappropriate content without unreasonably impacting teaching and learning.
- Has effective monitoring strategies in place that meets the College safeguarding needs

9. DIGITAL AND SECURITY STANDARDS

The Head of Digital Services is responsible for College's Cyber security governance which is aligned with the DfE's Cyber security: core standard**.** These standards require us to produce risk assessments, termly reviews, use MFA, carry out timely patching, have a good backup routine, use firewall protection and have some sort of monitoring and incident response for cyber attacks. All of these are in place and we are accredited with ISO27001 and Cyber Essentials awards.

10. GENERATIVE AI AND DYNAMIC CONTENT

We deploy 3 types of filter/cyber control on all our device. The first is a web-based filter which uses categories of site to limit access. The filter also logs and reports on every user that makes an internet connection through the College network.

The second is an alerting system which captures screen content and keystrokes to look for words or phrases. This should capture content classified as harmful such as instant messaging conversations. If an alert is triggered pastoral staff receive an email with a screenshot and can act on it instantly.

Finally, we have a security client on each machine which monitors the security stance of the machine and alerts if something flags (like malware, virus or an unexpected network connection). The alerts from this system go straight into Microsoft 365 and emails are sent to Digital Services staff who then respond.

11. ARTIFICIAL INTELLIGENCE AND EMERGING TECHNOLOGIES

College recognises the increasing risks presented by AI and emerging technologies, in particular those of generative AI, Deepfakes, Deepnudes and AI-generated abuse material. Staff and pupils received regular and updated education/training to alert them to both the risks and the technology itself.

12. ACCESS TO COLLEGE TECHNOLOGY

College provides internet, intranet and social media access and an email system to pupils and staff as well as other technology. Pupils and staff must comply with the respective Acceptable Use Policy when using College technology. All such use is monitored by the ICT Support Team.

Pupils and staff require individual usernames and passwords to access College internet, intranet and social media sites and email system which must not be disclosed to any other person. Any pupil or member of staff who has a problem with their usernames or passwords must report it to the ICT Support Team immediately.

Although pupils are issued with a College device as part of the one-to-one scheme, College also operates a BYOD policy for pupils who can log onto the College network with their devices via their College username and password. The use of any device connected to the College network will be logged and monitored by the ICT Support Team. See also below and the College Information Security Policy (including Remote Working and Bring Your Own Device to Work policy).

College has a separate Wi-Fi connection available for use by visitors to College. A password, which is changed on a regular basis, must be obtained from a member of staff in order to use the Wi-Fi. Use of this service will be logged and monitored by the Digital Services Department.

Use of mobile devices

College has appropriate filtering firewall and monitoring systems in place to protect pupils using the internet (including email text messaging and social media sites) when connected to the College network. These are provided by Watchguard; (https://www.watchguard.com/uk), with additional Safeguarding monitoring software provided by Smoothwall (https://www.smoothwall.com/education/)

Mobile devices equipped with a mobile data subscription can, however, provide pupils with unlimited and unrestricted access to the internet.

College rules about the use of mobile electronic devices, including access to open / non-College networks, are set out in the ICT Acceptable Use Policy for Pupils.

The use of mobile electronic devices by staff is covered in the Code of Conduct, IT
Acceptable Use Policy, Social Media Policy, Data Protection Policy for staff and Information Security Policy (including remote working and bring your own device to work). Personal mobile devices including laptop and notebook devices should not be used for School purposes except in an emergency.

College policies apply to the use of technology by staff and pupils whether on or off College premises and appropriate action will be taken where such use affects the welfare of other pupils or any member of the School community or where the culture or reputation of the College is put at risk.

13. PROCEDURES FOR DEALING WITH INCIDENTS OF MISUSE

Staff, pupils and parents are required to report incidents of misuse or suspected misuse to the College in accordance with this policy and College safeguarding and disciplinary policies and procedures.

Misuse by pupils
Anyone who has any concern about the misuse of technology by pupils should report it so that it can be dealt with in accordance with College's Behaviour, Discipline and Rewards Policy, including the Anti-Bullying and Anti-Cyber-Bullying Policy where there is an allegation of cyberbullying.

Anyone who has any concern about the welfare and safety of a pupil must report it immediately in accordance with College child protection procedures (see the College Safeguarding (Child Protection) policy).

It should be recognised that there are additional risks for students with the following profiles:

- SEND pupils
- LGBTQ+ pupils
- Pupils with mental health concerns
- Looked after children

Misuse by Staff
Anyone who has any concern about the misuse of technology by staff should report it in accordance with the College Whistleblowing Policy so that it can be dealt with in accordance with the staff disciplinary procedures.

If anyone has a safeguarding-related concern relating to staff misuse of technology, they should be report it immediately so that it can be dealt with in accordance with the procedures for reporting and dealing with allegations of abuse against staff set out in the College Safeguarding (Child Protection) policy.

Misuse by Any User
Anyone who has a concern about the misuse of technology by any other user should report it immediately to the Head of Digital Services or the Designated Safeguarding Lead.

College reserves the right to withdraw access to the College network by any user at any time and to report suspected illegal activity to the Police.

If College considers that any person is vulnerable to radicalisation College will refer this to the Channel programme. This focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Any person who has a concern relating to extremism may report it directly to the police.

14. EDUCATION

The safe use of technology is integral to the College curriculum. Pupils are educated in an age-appropriate manner about the importance of safe and responsible use of technology, including the internet, social media and mobile electronic devices (see the College Curriculum Policy).

The DSL is responsible for online pupil safety. Training of pupils is overseen by the Head of Wellbeing, working with the Head of Academic Digital Education and supported by the Head of Pastoral Care who manages the group of peer mentors called 'Cybirds'.

The safe use of technology is also a focus in all areas of the curriculum and key safety messages are reinforced as part of assemblies (Prayers)/ tutorial and Wellbeing activities, teaching pupils:

- about the risks associated with using the technology and how to protect themselves and their peers from potential risks;
- to be critically aware of content they access online and guided to validate accuracy of information;
- how to recognise suspicious, bullying or extremist behaviour;
- the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;
- the consequences of negative online behaviour; and
- how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how College will deal with those who behave badly.

The safe use of technology aspects of the curriculum are reviewed on a regular basis to ensure their relevance.

The College ICT Acceptable Use Policy for Pupils sets out the College rules about the use of technology including internet, email, social media and mobile electronic devices helping pupils to protect themselves and others when using technology. Pupils are reminded of the importance of this policy on an annual basis.

Useful online safety resources for pupils:
http://www.thinkuknow.co.uk/
http://www.childnet.com/young-people
https://www.saferinternet.org.uk/advice-centre/young-people https://www.disrespectnobody.co.uk/
http://www.safetynetkids.org.uk/
https://www.ceop.police.uk/Safety-Centre/How-can-CEOP-help-me-YP/

15. SAFEGUARDING

College's approach to online safety is reflected in the Safeguarding (Child Protection) Policy. Online safety is an integral part of safeguarding and is everyone's responsibility.

College considers the 4Cs detailed in the Safeguarding Policy (content, contact, conduct, commerce) provide the basis of an effective online policy. Both policies are also mindful of the emerging risks posed by sextortion and online coercion, financial exploitation, algorithmic radicalisation, misinformation, disinformation and conspiracy theories.

College has an ICT Acceptable Use Policy for pupils which recognises the use of mobile technology and that most pupils have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 4G and 5G). This access means some children, whilst at College may become involved in online sexual harassment, online harmful sexual behaviour, image-based abuse or child-on-child abuse. They may make, possess or share nude and semi-nude images. This behaviour is managed via these associated policies together with the Behaviour, Discipline and Rewards Policy. In addition, pupils with the College issued Surface Pros have the safeguarding monitoring software (Smoothwall), pre-installed and their activity will be monitored with significant alerts passed through to the DSL team.

College Council via the DSL and Digital Services Department will ensure online safety is a running theme in the whole College approach to safeguarding and related policies and procedures.

Remote education remains a means of learning for a small minority of pupils. College will be in touch with the parents of these pupils and communications reinforce the importance of children being safe online and help parents understand what College systems are in place what to filter and monitor online use. It will be especially important for parents to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from College their child is going to be interacting with online.

College Council via the DSL and Digital Services Department will ensure College has appropriate filters and monitoring systems in place which are reviewed regularly for their effectiveness.

16. TRAINING

Staff

College provides training on the safe use of technology to staff so that they are aware of how to protect pupils and themselves from the risks of using

technology and to deal appropriately with incidents involving the use of technology when they occur.
Induction training for new staff includes training on the College online safety strategy including this Policy, the Staff Code of Conduct and the IT Acceptable Use Policy for Staff. Ongoing staff development training includes training on technology safety together with specific safeguarding issues including filtering systems, monitoring systems, emerging technologies and AI-related risk, particularly sharing nudes and semi-nudes, generative AI, cyberbullying and radicalisation.

Staff also receive data protection training on induction and at regular intervals afterwards.

The frequency, level and focus of all such training will depend on individual roles and requirements and will be provided as part of College's overarching approach to safeguarding.

Useful online safety resources for staff:

- https://swgfl.org.uk/online-safety/
- https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals
- http://www.childnet.com/teachers-and-professionals
- https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
- https://www.thinkuknow.co.uk/teachers/
- http://educateagainsthate.com/
- https://www.commonsense.org/education/
- Cyberbullying: advice for head teachers and school staff (DfE, November 2014)
- Advice on the use of social media for online radicalisation (DfE and Home Office, July 2015)
- Sharing nudes and semi-nudes: advice for educational settings December 2024
  Generative AI
- Online safety in schools and colleges: questions from the governing board (UKCCIS, 2016)
  DfE Filtering and Monitoring Standards for Schools and Colleges updated June 2026 - Meeting Digital and Technology standards in Schools
  Cyber Security Standards for Schools and Colleges - Meeting Digital and Technology Standards in Schools
  Technology, planning and cyber security - Meeting the Cybersecurity Standards
  https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges
  Online – misinformation, disinformation and conspiracy theories - Pears Foundation
  Educate against Hate
  Countering Conspiracy theories

- Education for a connected world framework (UKCCIS)
- https://www.lgfl.net/online-safety/resource-centre

- Online Sexual Harassment: Understand, Prevent and Respond Guidance for Schools (Childnet, March 2019)
- SELMA Hack online hate toolkit (SWGFL, May 2019)
- Professionals online safety helpline: helpline@saferinternet.org.uk, 0344 381 4772.
- NSPCC helpline for anyone worried about a child - 0808 800 5000

The Gloucestershire Safeguarding Children's Partnership (GSCP) and Gloucestershire Safeguarding Education Partnership (GSEP) has produced guidance for professionals who work with children, young people and parents which is available here: I work with children, young people and parents - Safeguarding Children in Gloucestershire

Parents

College will provide regular parental guidance including communication about emerging risks through AI and emerging technologies. Parents will be provided with information sessions and opportunities to increase their understanding of AI and awareness of social media.

Parents are encouraged to read the ICT Acceptable Use Policy for Pupils with their child to ensure that it is fully understood.

Useful online safety resources for parents:

- https://www.saferinternet.org.uk/advice-centre/parents-and-carers
- http://www.childnet.com/parents-and-carers
- https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
- https://www.thinkuknow.co.uk/parents/
- http://parentinfo.org/
- http://parentzone.org.uk/
- https://www.net-aware.org.uk
- https://www.internetmatters.org/
- https://www.commonsensemedia.org/
- Advice for parents and carers on cyberbullying (DfE, November 2014).
- http://www.askaboutgames.com
- https://www.ceop.police.uk/safety-centre

17. RISK ASSESSMENT

Where a concern about a pupil's welfare is identified, the risks to that pupil's welfare will be assessed and appropriate action will be taken to reduce the risks identified. The concern must be referred to the DSL team immediately and the concerns recorded on CPOMS.

The format of risk assessment may vary and may be included as part of the College's overall response to a welfare issue, including the use of individual pupil welfare plans (such as behaviour, healthcare and education plans, as appropriate). Regardless of the form used, College approach to promoting pupil welfare will be systematic and pupil focused.

It is recognised that online activity may contribute to a pupil's vulnerability with regards anxiety, depression, eating disorders, self-harm, suicidal ideation or unhealthy comparison.

The Head of College has overall responsibility for ensuring that matters which affect pupil welfare are adequately risk assessed and for ensuring that the relevant findings are implemented, monitored and evaluated.

Day to day responsibility to carry out risk assessments under this policy will be delegated to the Designated Safeguarding Lead, Miss Caroline Ralph, who has been properly trained in, and tasked with, carrying out the particular assessment.

18. RECORD KEEPING

- All records created in accordance with this policy are managed in accordance with College policies that apply to the retention and destruction of records.
- All serious incidents involving the use of technology will be logged centrally in the technology incident log by the Head of Digital Services.
- The records created in accordance with this policy may contain personal data. College has a number of privacy notices which explain how College will use personal data about pupils and parents. The privacy notices are published on the College website. In addition, staff must ensure that they follow College data protection policies and procedures when handling personal data created in connection with this policy. This includes the College data protection policy and information security policy.