

Online Safety Policy

Reviewed by: Community and Wellbeing

Reviewed: November 2025

Contents

1.0 Aims	2
2.0 The four key categories of risk	2
3.0 Legislation and guidance.....	2
4.0 Roles and responsibilities	3
5.0 Educating pupils about online safety.....	7
6.0 Educating parents/carers about online safety	9
7.0 Cyber-bullying	10
8.0 Examining electronic devices	11
9.0 Artificial intelligence (AI).....	12
10.0 Acceptable use of the internet in school	13
11.0 Pupils using mobile devices in school	13
12.0 Staff using work devices outside school	14
13.0 How the school will respond to issues of misuse.....	14
14.0 Training	15
15.0 Links with other policies	16
16.0 Monitoring arrangements	16
Appendix 1: Acceptable Use Agreement (pupils and parents/carers).....	17
Appendix 2: Acceptable Use Agreement (staff, trustees, volunteers and visitors)	18

1.0 Aims

1.1 Our school aims to:

- 1.1.1 Have robust processes in place to ensure the online safety of pupils, staff, volunteers and trustees
- 1.1.2 Identify and support groups of pupils that are potentially at greater risk of harm online than others
- 1.1.3 Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- 1.1.4 Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2.0 The four key categories of risk

2.1 Our approach to online safety is based on addressing the following categories of risk:

- 2.1.1 Content – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- 2.1.2 Contact – being subjected to harmful online interaction with other users, such as 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
- 2.1.3 Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- 2.1.4 Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

3.0 Legislation and guidance

3.1 This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

3.1.1 [Teaching online safety in schools](#)

3.1.2 Meeting digital and technology standards

3.1.3 [Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff](#)

3.1.4 [Relationships and sex education](#)

3.1.5 [Searching, screening and confiscation](#)

3.2 It also refers to the DfE's guidance on [protecting children from radicalisation](#).

3.3 It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

3.4 The policy also takes into account the National Curriculum computing programmes of study.

3.5 This policy complies with our funding agreement and articles of association.

4.0 Roles and responsibilities

4.1 The board of trustees

4.1.1 The board of trustees has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

4.1.2 The board of trustees will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

4.1.3 The board of trustees will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

4.1.4 The board of trustees will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

4.1.5 The board of trustees will make sure that the school teaches pupils how to keep themselves and others safe, including online.

4.1.6 The board of trustees will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

4.1.6.1 Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;

4.1.6.2 Reviewing filtering and monitoring provisions at least annually;

4.1.6.3 Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;

4.1.6.4 Having effective monitoring strategies in place that meet their safeguarding needs.

4.1.6.5 The trustee who oversees online safety is Simon Weston.

4.1.7 All trustees will:

4.1.7.1 Make sure they have read and understand this policy

4.1.7.2 Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

4.1.7.3 Make sure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures

4.1.7.4 Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

4.2 The headteacher

4.2.1 The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

4.3 The designated safeguarding lead (DSL)

4.3.1 Details of the school's Safeguarding Team are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

4.3.2 The Designated Safeguarding Lead takes lead responsibility for online safety in school, in particular:

- 4.3.2.1 Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- 4.3.2.2 Working with the headteacher and board of trustees to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- 4.3.2.3 Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- 4.3.2.4 Providing trustees with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- 4.3.2.5 Working with the ICT manager to make sure the appropriate systems and processes are in place
- 4.3.2.6 Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- 4.3.2.7 Managing all online safety issues and incidents in line with the school's child protection policy
- 4.3.2.8 Responding to safeguarding concerns identified by filtering and monitoring
- 4.3.2.9 Making sure that any online safety incidents are logged via Class Charts Safeguarding and dealt with appropriately in line with this policy
- 4.3.2.10 Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- 4.3.2.11 Updating and delivering staff training on online safety
- 4.3.2.12 Liaising with other agencies and/or external services if necessary
- 4.3.2.13 Providing regular reports on online safety in school to the headteacher and/or governing board
- 4.3.2.14 Undertaking annual risk assessments that consider and reflect the risks children face
- 4.3.2.15 Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

4.3.3 This list is not intended to be exhaustive.

4.4 The IT manager

4.4.1 The IT manager is responsible for:

- 4.4.1.1 Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- 4.4.1.2 Making sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- 4.4.1.3 Implementing and developing a secure by design school's ICT system, through a security/safety-based approach
- 4.4.1.4 Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- 4.4.1.5 Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy

4.4.2 This list is not intended to be exhaustive.

4.5 All staff and volunteers

- 4.5.1 All staff, including contractors and agency staff, and volunteers are responsible for:
 - 4.5.1.1 Maintaining an understanding of this policy
 - 4.5.1.2 Implementing this policy consistently
 - 4.5.1.3 Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and making sure that pupils follow the school's terms on acceptable use (appendix 1)
 - 4.5.1.4 Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by speaking with a member of the safeguarding team and logging the concern via Class Charts Safeguarding.
 - 4.5.1.5 Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
 - 4.5.1.6 Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
 - 4.5.1.7 Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

4.5.2 This list is not intended to be exhaustive.

4.6 Parents/carers

4.6.1 Parents/carers are expected to:

4.6.1.1 Notify a member of staff or the headteacher of any concerns or queries regarding this policy

4.6.1.2 Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

4.6.1.3 Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

4.6.1.3.1 What are the issues? – [UK Safer Internet Centre](#)

4.6.1.3.2 Help and advice for parents/carers – [Childnet](#)

4.6.1.3.3 Parent and carers resource sheet – [Childnet](#)

4.7 Visitors and members of the community

4.7.1 Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

5.0 Educating pupils about online safety

5.1 Pupils will be taught about online safety as part of the curriculum:

5.2 The text below is taken from the [National Curriculum computing programmes of study](#) and the government's [guidance on relationships education, relationships and sex education \(RSE\) and health education \(for teaching until 31 August 2026\)](#).

5.2.1 All schools have to teach:

5.2.1.1 [Relationships and sex education and health education](#) in secondary schools

5.2.2 In **KS3**, pupils will be taught to:

5.2.2.1 Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy

5.2.2.2 Recognise inappropriate content, contact and conduct, and know how to report concerns

5.2.3 Pupils in **KS4** will be taught:

5.2.3.1 To understand how changes in technology affect safety, including new ways to protect their online privacy and identity

5.2.3.2 How to report a range of concerns

5.2.4 By the end of secondary school, pupils will know:

5.2.4.1 Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online

5.2.4.2 About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online

5.2.4.3 Not to provide material to others that they would not want shared further and not to share personal material that is sent to them

5.2.4.4 What to do and where to get support to report material or manage issues online

5.2.4.5 The impact of viewing harmful content

5.2.4.6 That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners

5.2.4.7 That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail

5.2.4.8 How information and data is generated, collected, shared and used online

5.2.4.9 How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

5.2.4.10 How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

5.2.4.11 The similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including through setting unrealistic expectations for body image), how people may curate a specific image of their life online, over-reliance on online relationships including social media, the risks related to online gambling including the accumulation of debt, how advertising and information is targeted at them and how to be a discerning consumer of information online, The safe use of social media and the internet will also be covered in other subjects where relevant.

5.2.4.12 Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5.3 Pupils will be taught practical cyber security skills

5.3.1 All pupils will receive age-appropriate training on safe internet use, including:

5.3.1.1 Methods that hackers use to trick people into disclosing personal information

5.3.1.2 Password security

5.3.1.3 Social engineering

5.3.1.4 The risks of removable storage devices (e.g. USBs)

5.3.1.5 Multi-factor authentication

5.3.1.6 How to report a cyber incident or attack

5.3.1.7 How to report a personal data breach

5.3.2 Pupils will also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

6.0 Educating parents/carers about online safety

6.1 The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

6.2 Online safety will also be covered during parents' evenings.

6.3 The school will let parents/carers know:

6.3.1 What systems the school uses to filter and monitor online use

6.3.2 What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

6.3.3 If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

6.3.4 Concerns or queries about this policy can be raised with any member of staff or the headteacher.

7.0 Cyber-bullying

7.1 Definition

7.1.1 Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

7.2 Preventing and addressing cyber-bullying

7.2.1 To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

7.2.2 The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors will discuss cyber-bullying with their tutor groups.

7.2.3 Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

7.2.4 All staff, trustee and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

7.2.5 The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

7.2.6 In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Anti-bullying policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

7.2.7 The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

8.0 Examining electronic devices

8.1 The headteacher, and any member of staff authorised to do so by the headteacher (as set out in our Searching and Confiscation Policy), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

8.1.1 Poses a risk to staff or pupils, and/or

8.1.2 Is identified in the school rules as a banned item for which a search can be carried out, and/or

8.1.3 Is evidence in relation to an offence

8.2 Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

8.2.1 Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Safeguarding Team.

8.2.2 Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it

8.2.3 Seek the pupil's co-operation

8.2.4 Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

8.3 When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

8.3.1 Cause harm, and/or

8.3.2 Undermine the safe environment of the school or disrupt teaching, and/or

8.3.3 Commit an offence

8.3.4 If inappropriate material is found on the device, it is up to the DSL/DDSL and the key stage lead to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

8.4 When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

8.4.1 They reasonably suspect that its continued existence is likely to cause harm to any person, and/or

8.4.2 The pupil and/or the parent/carer refuses to delete the material themselves

8.5 If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

8.5.1 Not view the image

8.5.2 Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

8.6 Any searching of pupils will be carried out in line with:

8.6.1 The DfE's latest guidance on [searching, screening and confiscation](#)

8.6.2 UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

8.6.3 Our Searching and confiscation policy

8.7 Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

9.0 Artificial intelligence (AI)

9.1 Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

9.2 Katharine Lady Berkeley's School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

9.3 Katharine Lady Berkeley's School will treat any use of AI to bully pupils very seriously, in line with our Anti-bullying policy.

9.4 Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school

9.5 Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

10.0 Acceptable use of the internet in school

10.1 All pupils, parents/carers, staff, volunteers and trustees are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

10.2 Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

10.3 We will monitor the websites visited by pupils, staff, volunteers, trustees and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

10.4 More information is set out in the acceptable use agreements in appendices 1 and 2.

11.0 Pupils using mobile devices in school

11.1 Pupils may bring mobile devices into school, but are not permitted to use them during the school day:

11.1.1 Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

11.1.2 Any breach of the acceptable use agreement by a pupil may lead to disciplinary action in line with the school behaviour and discipline policy, which may result in the confiscation of their device.

12.0 Staff using work devices outside school

12.1 All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

12.1.1 Keeping the device password-protected – strong passwords can be made up of [3 random words](#), in combination with numbers and special characters if required, or generated by a password manager

12.1.2 Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device

12.1.3 Making sure the device locks if left inactive for a period of time

12.1.4 Not sharing the device among family or friends

12.1.5 Installing anti-virus and anti-spyware software

12.1.6 Keeping operating systems up to date by always installing the latest updates

12.1.7 Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 2.

12.1.8 Work devices must be used solely for work activities.

12.1.9 If staff have any concerns over the security of their device, they must seek advice from the IT Manager

13.0 How the school will respond to issues of misuse

13.1 Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Internet acceptable use policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

13.2 Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

13.3 The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

14.0 Training

14.1 All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

14.2 All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

14.3 By way of this training, all staff will be made aware that:

14.3.1 Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

14.3.2 Children can abuse their peers online through:

14.3.3 Abusive, threatening, harassing and misogynistic messages

14.3.4 Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups

14.3.5 Sharing of abusive images and pornography, to those who don't want to receive such content

14.3.6 Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

14.4 Training will also help staff:

14.4.1 Develop better awareness to assist in spotting the signs and symptoms of online abuse

14.4.2 Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks

14.4.3 Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

14.4.4 The DSLs and deputy will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

14.5 Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

14.6 Volunteers will receive appropriate training and updates, if applicable.

14.7 More information about safeguarding training is set out in our child protection and safeguarding policy.

15.0 Links with other policies

15.1 This online safety policy is linked to our:

15.1.1 Child Protection and Safeguarding Policy

15.1.2 Behaviour and Discipline Policy

15.1.3 Staff Code of Conduct

15.1.4 Data Protection Policy

15.1.5 Complaints procedure

15.1.6 Internet acceptable use policy

16.0 Monitoring arrangements

16.1 Staff log behaviour and safeguarding issues related to online safety on Class Charts Safeguarding, including the date, where the incident took place, a description of the incident and any action taken.

16.2 This policy will be reviewed every year by the Deputy Headteacher. At every review, the policy will be shared with the trustee board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Appendix 1: Acceptable Use Agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in this Acceptable Use Agreement. I understand that these rules are in place to help keep me and others safe, and to ensure I use technology responsibly and respectfully.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only.
- Only use school devices or systems when supervised by a teacher or with a teacher's clear permission
- Be responsible for the device I am using, treating it with care and reporting any damage immediately
- Keep my usernames and passwords safe and not share these with others
- Keep my personal information private at all times and never share my name, address or telephone number with anyone without the permission of my teacher or parent/carers
- Tell a teacher or another trusted adult straight away if I see anything online that makes me or someone else feel upset, uncomfortable, or unsafe
- Always log off or shut down devices properly when I've finished using them
- Understand that **inappropriate use may lead to being banned from using school ICT systems**

I will not:

- Try to access inappropriate websites, including but not limited to social networking sites, chat rooms, gaming platforms, streaming sites, or sites containing violent, extremist or explicit content
- Open attachments or follow links in external emails without checking with a teacher
- Use inappropriate, offensive or abusive language in any online communication, including emails
- Create, link to, download or post material that is pornographic, obscene, offensive, threatening or illegal
- Log in to the school network using another person's username or password
- Arrange to meet someone offline without parental/carers knowledge and permission, or without adult supervision
- Use school email accounts to set up social media, online services or third-party accounts

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it whilst on the school site, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carers' agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carers):

Date:

Appendix 2: Acceptable Use Agreement (staff, trustees, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, TRUSTEES, VOLUNTEERS AND VISITORS

Name of staff member/trustee/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

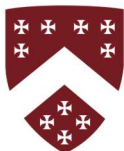
- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way that could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

- I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.
- I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.
- I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
- I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):

Date:

KLB



Katharine Lady Berkeley's School
Wotton-under-Edge, Gloucester, GL12 8LX

Tel: 01453 842227

Mail: info@klbschool.org.uk

www.klbschool.org.uk