Excalibur Academies Trust

Online Safety Policy

Version	Author	Created	Updated
1.2024	Fliss Hawkins	November 2024	

Date of approval	Approved by	Last Review date	Next Review date
04.11.2024	Core Executive Team		November 2026

Document Control Page

Revision	Date	Change	Origin of Change

Other Policies and Documents Associated
Child protection and safeguarding policy Behaviour policy Staff disciplinary procedures Data protection policy and privacy notices Complaints procedure ICT and internet acceptable use policy

Contents

1. 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 governors.

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

1.2 The 4 key categories of risk

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

1.2.1.1 Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism;

1.2.1.2 Contact – being subjected to harmful online interaction with other users, such as child-to-child 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;

1.2.1.3 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

1.2.1.4 Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

2. Legislation and guidance

2.1 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:

2.1.1 Teaching online safety in schools;

2.1.2 Preventing and tackling bullying and cyber-bullying: advice for headteacher/principal s and school staff;

2.1.3 [Relationships and sex education – remove if not applicable, see section 4];

2.1.4 Searching, screening and confiscation;

2.1.5 It also refers to the DfE's guidance on protecting children from radicalisation;

2.1.6 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;

2.2 The policy also considers the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Trust Board

3.1.1 The trust board has overall responsibility for monitoring this policy and holding the Executive Team to account for its implementation. The trust Board oversees online safety through its committee structure.

3.1.2 The Executive Team will ensure that staff undertake their mandatory training as per the mandatory training guidance which includes online safety training.

3.1.3 The governing board will co-ordinate meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety trends and patterns as provided by the designated safeguarding lead (DSL).

3.1.4 The Executive Team should ensure children are taught how to keep themselves and others safe, including keeping safe online.

3.1.5 The Trust Board will assure themselves that the Executive Team ensure that there are appropriate filtering and monitoring systems in place on devices and networks and regularly review their effectiveness. The board will assure themselves that the Executive Team are reviewing and implementing the DfE filtering and monitoring standards, which include:

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

3.1.5.2 Reviewing filtering and monitoring provisions at least annually;

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

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

3.1.5.5 Ensure 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.

3.2 The headteacher/principal

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

3.3 The designated safeguarding lead (DSL)

3.3.1 Details of the school's designated safeguarding lead (DSL) and deputy/deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

3.3.2 The DSL takes lead responsibility for online safety in school, in particular:

3.3.2.1 Supporting the headteacher/principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school;

3.3.2.2 Working with the headteacher/principal and governing board to review this policy every two years and ensure the procedures and implementation are updated and reviewed regularly;

3.3.2.3 Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks;

3.3.2.4 Working with the ICT manager to make sure the appropriate systems and processes are in place;

3.3.2.5 Working with the headteacher/principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents;

3.3.2.6 Managing all online safety issues and incidents in line with the school's child protection policy;

3.3.2.7 Ensuring that any online safety incidents are logged on cpoms and dealt with appropriately in line with this policy;

3.3.2.8 Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy;

3.3.2.9 Updating and delivering staff training on online safety;

3.3.2.10 Liaising with other agencies and/or external services if necessary;

3.3.2.11 Providing regular reports on online safety in school to the headteacher/principal and/or governing board. This includes reviews and checks alongside IT services to review filtering and monitoring and the 360-review tool from SWGfL;

3.3.2.12 Undertaking annual risk assessments that consider and reflect the risks children face. There will be a trust-wide risk assessment available;

3.3.2.13 Providing regular safeguarding and child protection updates, including online safety, to all staff, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

3.3.3 This list is not intended to be exhaustive.

3.4 The ICT manager

3.4.1 The ICT manager is responsible for:

3.4.1.1 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 ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material;

3.4.1.2 Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;

3.4.1.3 Conducting a full security check and monitoring the school's ICT systems on a regular basis;

3.4.1.4 Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;

3.4.1.5 Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy;

3.4.1.6 Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy and child-on-child processes.

3.4.2 This list is not intended to be exhaustive.

3.5 All staff and volunteers

3.5.1 All staff, including contractors and agency staff, and volunteers are responsible for:

3.5.1.1 Maintaining an understanding of this policy;

3.5.1.2 Implementing this policy consistently;

3.5.1.3 Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (see the Excalibur Employment manual and appendices 3) and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2);

3.5.1.4 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 informing the DSL;

3.5.1.5 Following the correct procedures, by emailing the IT helpdesk, if they need to bypass the filtering and monitoring systems for educational purposes;

3.5.1.6 Working with the DSL to ensure that any online safety incidents are logged on cpoms and dealt with appropriately in line with this policy;

3.5.1.7 Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy and child-on-child processes;

3.5.1.8 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';

3.5.2 This list is not intended to be exhaustive.

3.6 Parents/carers

3.6.1 Parents/carers are expected to:

3.6.1.1 Notify a member of staff or the headteacher/principal of any concerns or queries regarding this policy;

3.6.1.2 Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2);

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

3.6.2.1 What are the issues? – UK Safer Internet Centre;

3.6.2.2 Hot topics – Childnet;

3.6.2.3 Parent resource sheet – Childnet;

3.7 Visitors and members of the community

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 as outlined in our volunteer processes.

4. Educating pupils about online safety

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

4.1.1 The text below is taken from the National Curriculum computing programmes of study.

4.1.2 It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

4.2 All schools must teach:

4.2.1 Relationships education and health education in primary schools.

4.2.2 Relationships and sex education and health education in secondary schools.

Primary schools insert:

4.3 In Key Stage (KS) 1, pupils will be taught to:

4.3.1 Use technology safely and respectfully, keeping personal information private.

4.3.2 Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

4.4 Pupils in Key Stage (KS) 2 will be taught to:

4.4.1 Use technology safely, respectfully and responsibly.

4.4.2 Recognise acceptable and unacceptable behaviour.

4.4.3 Identify a range of ways to report concerns about content and contact.

4.5 By the end of primary school, pupils will know:

4.5.1 That people sometimes behave differently online, including by pretending to be someone they are not.

4.5.2 That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous.

4.5.3 The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.

4.5.4 How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.

4.5.5 How information and data is shared and used online.

4.5.6 What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).

4.5.7 How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

Secondary schools insert:

4.6 In KS3, pupils will be taught to:

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

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

4.7 Pupils in KS4 will be taught to:

4.7.1 Understand how changes in technology affect safety, including new ways to protect their online privacy and identity.

4.7.2 How to report a range of concerns.

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

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

4.8.2 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.

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

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

4.8.5 The impact of viewing harmful content.

4.8.6 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.

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

4.8.8 How information and data is generated, collected, shared and used online.

4.8.9 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.

4.8.10 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).

All schools – adapt this to reflect your school's approach:

4.9 The safe use of social media and the internet will also be covered in other subjects where relevant such as PHSE.

4.10 Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND. This may include the use of assemblies.

5. Educating parents/carers about online safety

5.1 The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE). This policy will also be shared with parents/carers via the website.

5.2 The school will let parents/carers know:

5.2.1 What systems the school uses to filter and monitor online use. This can be found on the school's website.

5.2.2 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.

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

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

6. Cyber-bullying

6.1 Definition

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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

6.2.1 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.

6.2.2 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. Class teachers will discuss cyber-bullying with their class.

6.2.3 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.

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

6.2.5 The school may also send information 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.

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

6.2.7 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.

6.3 Examining electronic devices.

6.3.1 The headteacher/principal, and any member of staff authorised to do so by the headteacher/principal (as set out in your behaviour policy) can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

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

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

6.3.1.3 Is evidence in relation to an offence.

Please refer to the behaviour policy for searching and confiscation procedures.

6.3.2 If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher/principal / other member of the

senior leadership team 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.

6.3.3 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:

6.3.3.1 Not view the image;

6.3.3.2 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.

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

6.3.4.1 The DfE's latest guidance on searching, screening and confiscation;

6.3.4.2 UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people;

6.3.4.3 Our behaviour policy / searches and confiscation procedures.

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

6.4 Artificial intelligence (AI)

6.4.1 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 Bard.

6.4.2 Excalibur 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.

6.4.3 Excalibur will treat any use of AI to bully pupils in line with our behaviour policy and child-on-child procedures.

7. Acceptable use of the internet in school

7.1 All pupils, parents/carers, staff, volunteers and governors 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. N.B. Please reference the Excalibur manual for the code of conduct relating to staff.

7.2 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.

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

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

8. Pupils using mobile devices in school

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

8.1.1 Lessons unless for medical purposes;

8.1.2 Clubs before or after school, or any other activities organised by the school.

8.2 Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

8.3 Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

Please refer to the Excalibur employment manual

10. How the school will respond to issues of misuse

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

10.2 The school will report to the police incidents which involve illegal activity or content, or otherwise serious circumstances.

11. Training

11.1 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.

11.2 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).

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

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

11.3.2 Children can abuse other children online through:

11.3.2.1 Abusive, threatening, harassing and misogynistic messages.

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

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

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

11.3.4 Training will also help staff:

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

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

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

11.3.5 The DSL and wider safeguarding team will undertake child protection and safeguarding training, which will include online safety, at least every 2 years provided by the local authority. They will also update their knowledge and skills about online safety at regular intervals.

11.3.6 Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training within academy committee meetings.

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

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

12. Monitoring arrangements

12.1 The DSL logs behaviour and safeguarding issues related to online safety.

12.2 This policy will be reviewed every two years by the Head of Safeguarding. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment produced by the central team 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.

13. Online Safety Signposting

Childnet – Provides guidance for schools on cyberbullying.

Educateagainsthate – Provides practical advice and support on protecting children from extremism and radicalisation.

London Grid for Learning – Provides advice on all aspects of a school or college's online safety arrangements.

NSPCC E-safety for schools – Provides advice, templates, and tools on all aspects of a school or college's online safety arrangements.

Safer recruitment consortium – 'Guidance for safe working practice', which may help ensure staff behaviour policies are robust and effective.

Searching screening and confiscation – Departmental advice for schools on searching children and confiscating items such as mobile phones.

South West Grid for Learning – Provides advice on all aspects of a school or college's online safety arrangements.

Use of social media for online radicalisation – A briefing note for schools on how social media is used to encourage travel to Syria and Iraq.

Online Safety Audit Tool – From UK Council for Internet Safety to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring.

Online safety guidance if you own or manage an online platform – DCMS advice.

A business guide for protecting children on your online platform – DCMS advice.

UK Safer Internet Centre – Provides tips, advice, guides and other resources to help keep children safe online.

13.1 Online safety relating to remote education, virtual lessons and live streaming

Guidance Get help with remote education – Resources and support for teachers and school leaders on educating pupils and students.

Departmental guidance on safeguarding and remote education – Including planning remote education strategies and teaching remotely.

London Grid for Learning – Guidance, including platform-specific advice.
National Cyber Security Centre – Guidance on choosing, configuring and deploying video conferencing.

UK Safer Internet Centre – Guidance on safe remote learning.

13.2 Online Safety-support for children

Childlinehttps://www.childline.org.uk/?utm_source=google&utm_medium=cpc&utm_campaign=UK_GO_S_B_BND_Grant_Childline_Information&utm_term=role_of_childline&gclsrc=aw.ds&&gclid=EAIaIQobChMIlfLRh-ez6AIVRrDtCh1N9QR2EAAYASAAEgLc-vD_BwE&gclsrc=aw.ds – For free and confidential advice.

UK Safer Internet Centre – To report and remove harmful online content.

CEOP – For advice on making a report about online abuse.

13.3 Online Safety-parental support

Childnet – Offers a toolkit to support parents and carers of children of any age to start discussions about their online life, and to find out where to get more help and support.

Commonsensemedia – Provides independent reviews, age ratings, & other information about all types of media for children and their parents.

Government advice – About protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying.

Internet Matters – Provides age-specific online safety checklists, guides on how to set parental controls, and practical tips to help children get the most out of their digital world How Can I Help My Child? – Marie Collins Foundation – Sexual abuse online.

London Grid for Learning – Provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online.

Stopitnow resource from The Lucy Faithfull Foundation – Can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online).

National Crime Agency/CEOP Thinkuknow – Provides support for parents and carers to keep their children safe online.

Parentzone – Provides help for parents and carers on how to keep their children safe online.

Talking to your child about online sexual harassment: A guide for parents – This is the Children's Commissioner's parental guide on talking to their children about online sexual harassment.

Report Harmful Content - We Help You Remove Content can help you to report harmful content online by providing up to date information on

community standards and direct links to the correct reporting facilities across multiple platforms.

Appendix 1: EYFS and KS1 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:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  o I select a website by mistake
  o I receive messages from people I don't know
  o I find anything that may upset or harm me or my friends
• Use school computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
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/carer 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 will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2, KS3, KS4 and KS5 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 the acceptable use agreement policy. **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 them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material that might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity in a safe and appropriate way. • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • The school will be informed by a parent/career that a device is needed. • The device will be switched off handed into the office, unless needed for medical purposes, and collected at the end of the school day. • If I am attending an after school club or activity the device will be collected from the office and handed over to the activity leader. • Should I need the device for medical purposes a risk assessment will be put in place around its use **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/carer's 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/carer):	**Date:**

Appendix 3: Staff, Governors, Volunteers and Visitors

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

When using the school's IT systems and accessing the internet in school, or outside school on a work device (if applicable), I will abide and follow the requirements set out in the Trust's IT acceptable use policy and employment manual (if applicable):

Leaving work laptop/computer/I-pad:
If you leave the IT device that you are using for any period of time you should take appropriate action and, in particular, you should log off or lock your device so that a password is required to gain access again.

Concerns:
You have a duty to report any concerns about the use of IT to the DSL/ Principal. For example, if you have a concern about IT security or pupils accessing inappropriate material.

Other policies: This policy should be read alongside the following:

- Code of Conduct;
- Data protection policy for Staff;
- Information security policy; and
- Acceptable use policy for pupils.

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 which 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

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF MEMBERS,GOVERNORS, VOLUNTEERS AND VISITORS	
Staff member, governor, volunteer, visitor agreement: • 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 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 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 inform me they have found any material which 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:**