



Online Safety Policy

Written By	Senior Leadership Team Computing Lead	
Frequency of Review	2 years	
Date reviewed and approved by Governing Body	Summer 2026	
Date of next review	Summer 2028	
Display on Website	✓	
Purpose	Outlines the safeguards and precautions in place in school to ensure safe internet access for our children at all times.	
Consultation	Governors	✓
	Parents	✓
	Pupils	✓
	Staff	✓
Links with other policies	Acceptable Usage Policy Accessibility Policy Anti-Bullying Policy Behaviour Policy Data Protection Policy Inclusion Policy Home Learning Policy Mobile Phone Policy Parent and Visitor Code of Conduct Safeguarding and Child Protection Policy Visitor Policy Charging policy Safeguarding Policy Preventing Radicalisation Policy	

Contents:

Statement of intent

1. [Legal framework](#)
2. [Roles and responsibilities](#)
3. [Managing online safety](#)
4. [Cyberbullying](#)
5. [Child-on-child sexual abuse and harassment](#)
6. [Grooming and exploitation](#)
7. [Mental health](#)
8. [Online hoaxes and harmful online challenges](#)
9. [Cyber-crime](#)
10. [Online safety training for staff](#)
11. [Online safety and the curriculum](#)
12. [Use of technology in the classroom](#)
13. [Use of smart technology](#)
14. [Educating parents](#)
15. [Internet access](#)
16. [Filtering and monitoring online activity](#)
17. [Network security](#)
18. [Emails](#)
19. [Generative artificial intelligence \(AI\)](#)
20. [Social networking](#)
21. [The school website](#)
22. [Use of devices](#)
23. [Remote learning](#)
24. [Monitoring and review](#)

Appendices

Appendix 1 Online harms and risks – curriculum coverage

Appendix 2 Burlington Junior School Acceptable Use Agreement for Parents

Appendix 3 Burlington Junior School Acceptable Use Agreement for Pupils

Appendix 4 Burlington Junior School Acceptable Use Agreement for Staff

Appendix 5 Videos games and keeping children safe for parents

Appendix 6 Device loan agreement

Statement of intent

Burlington Junior School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

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

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

1. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2023) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE Keeping children safe in education'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

2. Roles and responsibilities

The governing board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The headteacher will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the deputy DSL's by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.

- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and ICT technicians to conduct reviews of this policy as appropriate.
- Working with the DSL and governing board to update this policy on a bi-annual basis.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety.
- Working with the headteacher and ICT technicians to conduct light-touch reviews of this policy as appropriate.
- Working with the headteacher and governing board to update this policy on an bi-annual basis.

ICT technicians will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and headteacher to conduct light-touch reviews of this policy as appropriate

All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.

- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

3. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL will liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training.
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation.
- Online safety is integrated into learning throughout the curriculum.
- Assemblies are conducted termly on the topic of remaining safe online.
- We work in partnership with the Local Authority with regards to training and updates.
- Online safety is integrated into our safeguarding policy.

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also

acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the headteacher and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded by the DSL.

4. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging

- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

5. Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Behaviour Policy and Child Protection and Safeguarding Policy.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Behaviour Policy and the Child Protection and Safeguarding Policy.

6. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment,

e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Preventing Radicalisation Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Preventing Radicalisation Policy.

7. Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health.

8. Online hoaxes and harmful online challenges

For the purposes of this policy, an **“online hoax”** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **“harmful online challenges”** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

9. Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will liaise with the local authority to implement the appropriate course of action. This could involve a referral to the Cyber Choices Programme.

The headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

10. Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

11. Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- PSHE (through Relationships and Health Education)
- Computing

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in appendix A of this policy.

The school's approach to teaching online safety in the curriculum will reflect the ever-evolving nature of online risks, ensuring pupils develop the knowledge and resilience to navigate digital spaces safely and responsibly. Online safety education will address four key categories of risk: content, contact, conduct, and commerce.

Content Risks

Pupils will be taught how to critically evaluate online content and identify material that is illegal, inappropriate, or harmful. Lessons will equip pupils with the skills to question sources, verify information, and understand the dangers of engaging with such content.

Contact Risks

The school will educate pupils about the potential dangers of interacting with others online. They will learn how to recognise unsafe interactions, use privacy settings effectively, and report any concerning behaviour or messages to trusted adults and platforms.

Conduct Risks

Pupils will be guided on how their own online behaviour can impact both themselves and others. Online bullying, including the use of social media and messaging platforms to harass or intimidate others, will also be a key focus. Pupils will be taught responsible digital conduct and the legal and emotional consequences of harmful behaviour.

Commerce Risks

The curriculum will also include education on online commercial risks. Pupils will be informed about the exposure to inappropriate advertising, and financial scams such as phishing. They will learn how to recognise fraudulent schemes, protect their personal and financial information, and seek help when confronted with suspicious online activity.

The DSL will be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the computing lead and curriculum leader will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

12. Use of technology in the classroom

A wide range of technology will be used during lessons, including the following:

- Computers
- Laptops
- Chromebooks
- Tablets (iPads)
- Intranet
- Email
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

13. Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's Acceptable Use Agreement for Pupils.

Staff will use all smart technology and personal technology in line with the school's Staff Mobile Phone Policy.

The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school's acceptable use of ICT agreement for pupils.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Pupils **will not** be permitted to use smart devices or any other personal technology whilst in the classroom.

Where it is deemed necessary, the school will ban pupil's use of personal technology whilst on school site.

Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Behaviour Policy.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

14. Educating parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be sent a copy of the Acceptable Use Agreement when a child starts at Burlington Junior School and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Parents' evenings
- Newsletters
- Online resources

- Online safety workshops

15. Internet access

Pupils, staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record will be kept of users who have been granted internet access in the school office.

All members of the school community will be encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

16. Filtering and monitoring online activity

The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's ['Filtering and monitoring standards for schools and colleges'](#). The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The headteacher and ICT technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. ICT technicians will undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the headteacher. Prior to making any changes to the filtering system, ICT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT technicians. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Staff Code of Conduct.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are

monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

17. Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by ICT technicians. Firewalls will be switched on at all times. ICT technicians will review the firewalls on a regular basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks to ICT technicians.

All members of staff will have their own unique usernames and private passwords to access the school's systems. All pupils will be provided with their own unique username and private passwords. Staff members and pupils will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

Users will inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use.

18. Emails

Access to, and the use of, emails will be managed in line with the Data Protection Policy and the Acceptable Use Agreement.

Staff and pupils will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. School email accounts must be used to communicate with the school community. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members and pupils will be required to block spam and junk mail, and report the matter to ICT technicians. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened.

Computing lessons and assemblies will include information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use

- The importance of asking “does the email urge you to act immediately?”
- The importance of checking the spelling and grammar of an email

19. Generative artificial intelligence (AI)

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

20. Social networking

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the Acceptable Use Policy, which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13, but the school regularly deals with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that online harms regulation is likely to require more stringent age verification measures over the coming years.

The school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). You may wish to refer to the [Top Tips for Parents](#) poster along with relevant items from parentsafe.lgfl.net and introduce the [Children's Commission Digital 5 A Day](#).

The school does not have an official social media presence so no opinions or posts on social media will have been approved by Burlington Junior School.

Email to parent@burlingtonjunior.org is the official electronic communication channel between parents and the school. Electronic communication between staff and pupils will be carried out using school accounts for educational purposes only, through the following monitored platforms: Google classroom.

Pupils/students are not allowed to be 'friends'* with or make a 'friend request'** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils/students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

** Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher, and should be declared upon entry of the pupil or staff member to the school).*

*** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).*

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

All members of the school community are reminded that particularly in the context of social media, it is important to comply that permission is sought before uploading photographs, videos or any other information about other people.

The statements of the Acceptable Use Policies (AUPs) which all members of the school community have read are also relevant to social media activity, as is the school's Data Protection Policy.

21. The School Website

The headteacher will be responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

22. Use of Devices

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary. If the school supplies a Chromebook for pupils to use at home, the parent will need to sign a Loan Agreement (Appendix 9). The Chromebook will have security features from Google and monitoring software from Senso cloud. The Internet will not be filtered when used off-site and this will be the responsibility of the Parent.

The use of personal devices on the school premises and for the purposes of school work will be managed in line with the Acceptable Use Policy.

22.1 The use of digital images and video

To comply with the General Data Protection Regulation (which supersedes the 1998 Data Protection Act), we need your permission before we can photograph or make recordings of your daughter / son.

Burlington Junior School rules for any external use of digital images are:

- If the pupil is named, we avoid using their photograph.
- If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils' work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staff are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity, e.g. taking photos or a video of progress made in a lesson.
- Your child's image being used for presentation purposes around the school, e.g. in class or wider school wall displays or PowerPoint® presentations.
- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators, e.g. in our school prospectus or on our school website. On rare occasions, your child's picture could appear in the media if a newspaper photographer or

television film crew attends an event. Permission will always be sought in these circumstances.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if they won a national competition and wanted to be named in local or government literature.

23. Remote learning

All remote learning will be delivered in line with the school's Home Learning Policy which can be found on our school website.

Sometimes the school may have to switch to Remote learning. When this occurs these are steps we will take when undertaking live sessions (video calling):

- We will only use school-registered accounts, never personal ones.
- We will always have at least 2 staff members present on any live session with pupils.
- We will only use Google Meet as a live video platform and post web link in the Google Classroom.
- We will ensure all pupils are included and if possible, provide pupils with a device to use.
- We will turn off 'Quick Access' to Google Meet to prevent logins from outside the school community.
- We will discuss safety and etiquette when online with pupils: safe and appropriate place with no bedrooms or inappropriate objects/information visible
- We will avoid one-to-ones unless pre-approved by Senior Leadership Team
- We will discuss the ground rules in live sessions. – no recording of sessions, stay on mute, cameras on showing shoulders and head, use the raise hand button, chat used for learning purposes only.

For safeguarding concerns when online or Remote learning, we have 'Worry Buttons' in every pupil Google Classroom where they are able to report any concern they have to the Designated Safeguarding Leaders. Where members of staff have concerns during a period of remote learning, they should report online safety incidents in the same way as any safeguarding incident and report in line with school procedures (in line with recent updates and training).

If the school supplies a Chromebook for pupils to use at home, the parent will need to sign a Loan Agreement (Appendix 9). The Chromebook will have security features from Google and monitoring software from Securus XT. The Internet will not be filtered and this will be the responsibility of the Parent.

24. Monitoring and review

The school recognises that the online world is constantly changing; therefore, the DSL, the Computing Leader, ICT technicians and the headteacher conduct regular light-touch reviews of this policy to evaluate its effectiveness.

The governing board, headteacher and DSL will review this policy in full on a bi-annual basis and following any online safety incidents.

The next scheduled review date for this policy is September 2028.

Any changes made to this policy are communicated to all members of the school community.

Appendices

Appendix 1 Online harms and risks – curriculum coverage

Appendix 2 Burlington Junior School Acceptable Use Agreement for Parents

Appendix 3 Burlington Junior School Acceptable Use Agreement for Pupils

Appendix 4 Burlington Junior School Acceptable Use Agreement for Staff

Appendix 5 Device loan agreement

Online harms and risks – curriculum coverage

The table below contains information from the DfE's 'Teaching online safety in schools' guidance about what areas of online risk schools should teach pupils about.

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
How to navigate the internet and manage information		
Age restrictions	<p>Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching will include the following:</p> <ul style="list-style-type: none"> • That age verification exists and why some online platforms ask users to verify their age • Why age restrictions exist • That content that requires age verification can be damaging to under-age consumers • What the age of digital consent is (13 for most platforms) and why it is important 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE – Health Education • Computing
How content can be used and shared	<p>Knowing what happens to information, comments or images that are put online. Teaching will include the following:</p> <ul style="list-style-type: none"> • What a digital footprint is, how it develops and how it can affect pupils' futures • How cookies work • How content can be shared, tagged and traced • How difficult it is to remove something once it has been shared online • What is illegal online, e.g. youth-produced sexual imagery (sexting) 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE - Relationships education • Computing
Disinformation, misinformation and hoaxes	<p>Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching will include the following:</p> <ul style="list-style-type: none"> • Disinformation and why individuals or groups choose to share false information in order to deliberately deceive • Misinformation and being aware that false and misleading information can be shared inadvertently • Misinformation and understanding that some genuine information can be published with the deliberate intent to harm, e.g. releasing private information or photographs • Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE - Relationships and health education • Computing

	<ul style="list-style-type: none"> • That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online • How to measure and check authenticity online • The potential consequences of sharing information that may not be true 	
Fake websites and scam emails	<p>Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching will include the following:</p> <ul style="list-style-type: none"> • How to recognise fake URLs and websites • What secure markings on websites are and how to assess the sources of emails • The risks of entering information to a website which is not secure • What pupils should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email • Who pupils should go to for support • The risk of 'too good to be true' online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE - Relationships education • Computing
Online fraud	<p>Fraud can take place online and can have serious consequences for individuals and organisations. Teaching will include the following:</p> <ul style="list-style-type: none"> • What identity fraud, scams and phishing are • That online fraud can be highly sophisticated and that anyone can be a victim • How to protect yourself and others against different types of online fraud • How to identify 'money mule' schemes and recruiters • The risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal • The risk of sharing personal information that could be used by fraudsters • That children are sometimes targeted to access adults' data • What 'good' companies will and will not do when it comes to personal details • How to report fraud, phishing attempts, suspicious websites and adverts 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE - Relationships education • Computing

<p>Password phishing</p>	<p>Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching will include the following:</p> <ul style="list-style-type: none"> • Why passwords are important, how to keep them safe and that others might try to get people to reveal them • How to recognise phishing scams • The importance of online security to protect against viruses that are designed to gain access to password information • What to do when a password is compromised or thought to be compromised 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE - Relationships education • Computing
<p>Personal data</p>	<p>Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching will include the following:</p> <ul style="list-style-type: none"> • How cookies work • How data is farmed from sources which look neutral • How and why personal data is shared by online companies • How pupils can protect themselves and that acting quickly is essential when something happens • The rights children have with regards to their data • How to limit the data companies can gather 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE - Relationships education • Computing
<p>Persuasive design</p>	<p>Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching will include the following:</p> <ul style="list-style-type: none"> • That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible to encourage them to spend money or generate advertising revenue • How notifications are used to pull users back online 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE - Health education • Computing
<p>Privacy settings</p>	<p>Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching will include the following:</p> <ul style="list-style-type: none"> • How to find information about privacy settings on various sites, apps, devices and platforms • That privacy settings have limitations 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE - Relationships education • Computing
<p>Targeting of online content</p>	<p>Much of the information seen online is a result of some form of targeting. Teaching will include the following:</p>	<p>This risk or harm will be covered in the following curriculum areas:</p>

	<ul style="list-style-type: none"> • How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts • How the targeting is done • The concept of clickbait and how companies can use it to draw people to their sites and services 	<ul style="list-style-type: none"> • PSHE - Relationships education • Computing
How to stay safe online		
Online abuse	<p>Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching will include the following:</p> <ul style="list-style-type: none"> • The types of online abuse, including sexual harassment, bullying, trolling and intimidation • When online abuse can become illegal • How to respond to online abuse and how to access support • How to respond when the abuse is anonymous • The potential implications of online abuse • What acceptable and unacceptable online behaviours look like 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE - Relationships education • Computing
Radicalisation	<p>Pupils are at risk of accessing inappropriate and harmful extremist content online, including terrorist material. Extremist and terrorist groups use social media to identify and target vulnerable individuals. Teaching will include the following:</p> <ul style="list-style-type: none"> • How to recognise extremist behaviour and content online • Which actions could be identified as criminal activity • Techniques used for persuasion • How to access support from trusted individuals and organisations 	<p>All areas of the curriculum</p>
Challenges	<p>Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching will include the following:</p> <ul style="list-style-type: none"> • What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal • How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why • That it is okay to say no and to not take part in a challenge • How and where to go for help • The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE - Relationships education

<p>Content which incites violence</p>	<p>Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching will include the following:</p> <ul style="list-style-type: none"> • That online content (sometimes gang related) can glamorise the possession of weapons and drugs • That to intentionally encourage or assist in an offence is also a criminal offence • How and where to get help if they are worried about involvement in violence 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Relationships education
<p>Fake profiles</p>	<p>Not everyone online is who they say they are. Teaching will include the following:</p> <ul style="list-style-type: none"> • That, in some cases, profiles may be people posing as someone they are not or may be 'bots' • How to look out for fake profiles 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE - Relationships education • Computing
<p>Grooming</p>	<p>Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, gangs and financial exploitation. Teaching will include the following:</p> <ul style="list-style-type: none"> • Boundaries in friendships with peers, in families, and with others • Key indicators of grooming behaviour • The importance of disengaging from contact with suspected grooming and telling a trusted adult • How and where to report grooming both in school and to the police <p>At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.</p>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE - Relationships education
<p>Livestreaming</p>	<p>Livestreaming (showing a video of yourself in real-time online, either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching will include the following:</p> <ul style="list-style-type: none"> • What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content • That online behaviours should mirror offline behaviours and that this should be considered when making a livestream • That pupils should not feel pressured to do something online that they would not do offline • The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Computing

	<ul style="list-style-type: none"> • The risks of grooming 	
<p>Unsafe communication</p>	<p>Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching will include the following:</p> <ul style="list-style-type: none"> • That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with • How to identify indicators of risk and unsafe communications • The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before • What online consent is and how to develop strategies to confidently say no to both friends and strangers online 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Relationships education • Computing
Wellbeing		
<p>Impact on confidence (including body confidence)</p>	<p>Knowing about the impact of comparisons to 'unrealistic' online images. Teaching will include the following:</p> <ul style="list-style-type: none"> • The issue of using image filters and digital enhancement • The role of social media influencers, including that they are paid to influence the behaviour of their followers • That 'easy money' lifestyles and offers may be too good to be true • The issue of photo manipulation, including why people do it and how to look out for it 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE • Computing
<p>Impact on quality of life, physical and mental health and relationships</p>	<p>Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching will include the following:</p> <ul style="list-style-type: none"> • How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time) • How to consider quality vs. quantity of online activity • The need for pupils to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or due to the fear of missing out • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive • The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues • That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Health education

	<ul style="list-style-type: none"> • Where to get help 	
Online vs. offline behaviours	<p>People can often behave differently online to how they would act face to face. Teaching will include the following:</p> <ul style="list-style-type: none"> • How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressure How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE - Relationships education
Suicide, self-harm and eating disorders	<p>Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using language, videos and images.</p>	

Appendix 2 - Burlington Junior School Acceptable Use Agreement for Parents

Burlington Junior School regularly reviews and updates all Acceptable Use documents to ensure that they are consistent with the school Online Safety and Safeguarding Policies, which can be found on our school website. We attempt to ensure that all students have good access to digital technologies to support their teaching and learning. We expect all our students to agree to be responsible users to help keep everyone safe and to be fair to others.

Your child will be asked to read and sign an Acceptable Use Policy tailored to their age. Please read this carefully – it is available on our school website.

Parents' Acceptable Use Agreement

Internet and IT

As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my daughter / son access to:

- the internet at school
- the school's chosen email system
- blogging platforms (J2E)
- IT facilities and equipment at the school

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

I understand that all internet and devices used in school are subject to filtering and monitoring; I understand that all school-owned devices used outside of school may also be subject to filtering and monitoring, and should be used in the same manner as when in school.

Use of digital images, photography and video

I understand the school has a clear policy on "The use of digital images and video" and I support this.

I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.

I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.

Social networking and media sites: I understand that the school has a clear policy on "The use of social networking and media sites" and I support this. The impact of social media use is often felt in schools, and this is why we expect certain behaviours from pupils when using social media at all times.

I will not take and then share online, photographs, videos etc. about other children (or staff) at school events, without the school's permission.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I understand that my son/daughter has agreed in the pupil acceptable-use policy not to search for or share any material that could be considered offensive, harmful or illegal. This might include bullying or extremist/hate/discriminatory content.

I will support the school by promoting safe and responsible use of the internet, online services and digital technology at home. I will inform the school if I have any concerns.

Name(s) of pupil/student: _____ Class _____

Parent / guardian signature: _____

Date: ___/___/___

Appendix 3 - Burlington Junior School Acceptable Use agreement for pupils

This agreement will help keep me safe and help me to be fair to others.

- I am an online digital learner – I use the school’s internet and devices for schoolwork, homework and other activities to learn and have fun. I only use sites, games and apps that my trusted adults say I can.
- I am a secure online learner – I keep my passwords to myself and reset them if anyone finds them out.
- I am careful online – I think before I click on links and only download when I know it is safe or has been agreed by trusted adults. I understand that some people might not be who they say they are, so I should be very careful when someone wants to be my friend.
- I am private online – I only give out private information if a trusted adult says it’s okay. This might be my home address, phone number or other personal information that could be used to identify me or my family and friends.
- I keep my body to myself online – I never change what I wear in front of a camera and remember that my body is mine and mine only, and I don’t send any photos without checking with a trusted adult.
- I say no online if I need to – if I get asked something that makes me worried or upset or just confused, I say no, stop chatting and tell a trusted adult.
- I am a rule-follower online – I know that some websites and social networks have age restrictions and I respect this; I only visit sites, games and apps that my trusted adults have agreed to.
- I am considerate online – I do not join in with bullying or sharing inappropriate material.
- I am respectful online – I do not post, make or share unkind, hurtful or rude messages/comments and tell my trusted adults if I see these.
- I am part of a community – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
- I am responsible online – I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed or is worried or upset by things they read, watch or hear.
- I don’t do public live streams on my own – and only go on a video chat if my trusted adult knows I am doing it and who with.
- I communicate and collaborate online – with people I know and have met in real life or that a trusted adult knows about.
- I am SMART online – I understand that unless I have met people in real life, I can’t be sure who someone is online, so if I want to meet someone for the first time, I must always ask a trusted adult for advice.

- I am a creative digital learner online – I don't just spend time online to look at things from other people; I get creative to learn and make things! I only edit or delete my own digital work and only use other people's with their permission or where it is copyright free or has a Creative Commons licence.
- I am a researcher online – I use safer search tools approved by my trusted adults. I understand that not everything online can be believed, but I know how to check things and know to 'double check' information I find online.

I have read and understood this agreement. I know who are my trusted adults are and agree to the above.

Appendix 4 - Burlington Junior School Acceptable Use Agreement for Staff

Introduction

All staff and Governors wishing to use school Computing resources and systems need to sign a copy of the declaration contained in this document and return to the Headteacher, where it will be kept on file. If there are any concerns, access rights will be withdrawn. A record will be maintained of all users with system access. Users will be removed from this record when access is no longer required, in accordance with the Data Protection Act. Users will be advised of any changes made to these policies.

Acceptable Use Policy

The Computing facilities are owned by the school (this includes laptops allocated to individual staff) and their use is an entitlement for all authorised users, subject to the conditions set out below:

- All Computing based activity must be appropriate to a school environment
- Access to shared resources must be made via the user's authorised account and password
- Users will not disclose their account name and password to any other person
- Users will always log in using their own usernames and passwords
- It is forbidden to partake in any activity that threatens the integrity of the school's facilities, including the use of the internet to access inappropriate materials
- The school reserves the right to monitor the use of Computing resources, emails sent or received, files held and internet sites visited at any time, including examining and deleting any files held.
- Users must prepare the use of video clips and images to ensure they are appropriate before sharing with children
- Staff must always log off or lock any computer after use

By logging on to the school's computing resources all users agree to abide by the condition above and agree not to use them to:

- Access chat room services or download files from internet without express permission
- Publish information which could identify the user or any other person directly on any web page
- Send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.
- Upload, download or otherwise transmit commercial software or any copyrighted materials
- Introduce any form of computer virus into the network
- Transmit unsolicited commercial or advertising material
- Use the service to set up or run a personal business
- Post anonymous messages or send chain letters
- Broadcast unsolicited personal views on social, political or religious matters
- Represent personal opinions as those of the school or Local Authority
- Send pupil or staff data through unauthorised lockdowns

All users also agree to:

- Seek permission from the Headteacher or Subject Leader for Computing before downloading any software such as itunes/Spotify etc.
- Report any inadvertent access to inappropriate websites to members of the Senior Leadership Team

Transfer of Sensitive Data (GDPR)

We aim to produce guidelines for staff to minimise a breach of data during which sensitive data may be lost, become vulnerable, altered or stolen. Sensitive data is defined as any personal or confidential information that can be linked to a specific person.

With regards to sensitive data staff are expected to:

- Never create or store data which contains any client-specific information on personal devices, regardless of where they intend to use the data
- Only use password protected school supplied laptops or memory sticks should they need to transport sensitive data
- Only use approved cloud storage for sensitive data: MyDrive/USO FX2 on LGFL.net or Google drive
- Avoid the use laptops and memory sticks as a means of transporting data on a temporary basis and use a remote desktop connection to the school server to access files.
- Transport data to school storage facility and delete data from laptop or memory stick as soon as it is no longer needed
- Only take sensitive physical data (e.g. pupil file) home when absolutely necessary and with the express permission of the Headteacher
- Never leave sensitive data/files unattended
- Maintain the confidential nature of the data wherever that data may be e.g. car/home
- Never read or make notes on sensitive files during a journey on public transport (no labels visible)
- Never post images relating to school on internet or social networking

With regards to email staff are expected to be aware that:

- The content security and safe receipt of information sent by email is always the responsibility of the sender
- Emails can be the subject of interception
- Good practice includes the use of initials rather than names, dates of birth, addresses etc.
- Normal non-secure email may be used for day-to-day communication with colleagues, third parties and other agencies where the nature of the information is not confidential
- Any electronic communication between staff at school and the Local Authority which contains sensitive data should be made using a secure system called USO-FX or between Encrypted LGFLmail accounts.
- Anonymised information may be sent through normal email only when extra care has been taken to verify the recipient (e.g. telephone call)
- Pupil specific reports and documents should not be sent as an attachment to an email to anyone outside the Local Authority
- Emails should always be of a professional nature with due regard to the recipient
- Emails containing sensitive data and/or in connection with school matters should only be created by an appropriate member of staff.
- Sensitive data must only be sent via Atomwide by an appropriate member of staff.

Data Breaches:

On the discovery of a potential breach of data the matter should be referred immediately to the Headteacher. The Headteacher will then initiate an enquiry to ascertain the nature and scope of the breach. If it is believed that sensitive data may have been compromised then the Headteacher will notify the Local Authority or Information Commissioner's Office (ICO) and seek advice regarding subsequent action.

Online safety

Online Safety for pupils

All adults within the school are responsible for ensuring pupils are safe when using the internet. Teaching staff are required to teach Online Safety discretely in computing and PSHE lessons, and address it within other curriculum areas.

Staff should adhere to the information in this policy where there are any safeguarding concerns.

Online Safety for adults

In addition to the Acceptable Use and Data Protection policies, staff are required to use the computing facilities sensibly, lawfully and professionally. Staff should adhere to the information within the Online Safety Policy. Training in online safety will be provided at regular intervals for all staff.

Acceptable Usage Policy for staff

I confirm I have read the policy statements noted above and agree to abide by the conditions.

I understand that misuse of school’s computing equipment or systems is a serious offence and could lead to disciplinary procedures.

User’s Name _____

User’s signature_____

Appendix 5 - Device loan agreement.

Device loan agreement for pupils

1. This agreement is between:

1) Burlington Junior School, New Malden, KT3 4LT ("the school")

2) Name of parent: _____

Address: _____

("the parent" and "I")

And governs the use and care of devices assigned to the parent's child (the "pupil"). This agreement covers the period from the date the device is issued through to the return date of the device to the school.

All issued equipment shall remain the sole property of the school and is governed by the school's policies.

The school is lending the pupil a computer device ("the equipment") for the purpose of doing school work from home.

1. This agreement sets the conditions for taking a Burlington Junior School device ("the equipment") home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I and the pupil will adhere to the terms of loan.

2. Damage/loss

By signing this agreement I agree to take full responsibility for the loan equipment issued to the pupil and I have read or heard this agreement read aloud and understand the conditions of the agreement.

I understand that I and the pupil are responsible for the equipment at all times whether on the school's property or not.

If the equipment is damaged, lost or stolen, I will immediately inform the school, and I acknowledge that I am responsible for the reasonable costs requested by the school to repair or replace the equipment. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to the school on their demand from the school in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

I will make sure my child takes the following measures to protect the device:

- Keep the device in a secure place when not in use;
- Don't leave the device in a car or on show at home;
- Don't eat or drink around the device;
- Don't lend the device to friends;

- Don't leave the equipment unsupervised in unsecured areas.

3. Unacceptable use

I am aware that the school monitors the pupil's activity on this device.

I agree that my child will not carry out any activity that constitutes 'unacceptable use'.

This includes, but is not limited to the following:

- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Causing intentional damage to ICT facilities or materials
- Using inappropriate or offensive language

I accept that the school will sanction the pupil, in line with our Behaviour Policy, if the pupil engages in any of the above at any time.

4. Personal use

I agree that the pupil will only use this device for educational purposes and not for personal use and will not loan the equipment to any other person.

5. Data protection

- I agree to take the following measures to keep the data on the device protected.
- Keep the equipment password-protected - strong passwords with a combination of upper and lower-case letters, numbers;
- Make sure my child locks the equipment if it's left inactive for a period of time;
- Do not share the equipment among family or friends;
- Install the latest updates to operating systems, as prompted.

If I need help doing any of the above, I will contact the school on the email parent@bjs.rbksch.org

6. Return date

I will return the device in its original condition to the school office within 7 days of being requested to do so. I will ensure the return of the equipment to the school if the pupil no longer attends the school.

7. Consent

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

PUPIL'S FULL NAME
PARENT'S FULL NAME
PARENT'S SIGNATURE
DEVICE SERIAL NUMBER, MAKE AND MODEL