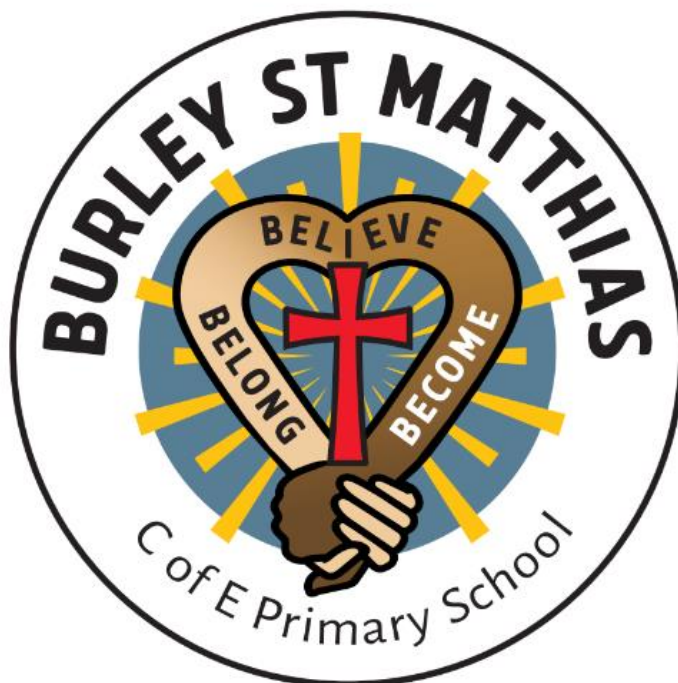




Burley St Matthias C of E Primary School

E-Safety Policy

2026

Date Policy Ratified	23.9.26
Date Policy Reviewed	23.9.27
Chair of Governors	Liz Powell and Hannah Bithell

Vision

As a loving church school at the heart of our community, we are a place where all are welcomed and cherished – a true sanctuary where everyone can **belong, believe and become**. Guided by our Christian values, we nurture each child to feel valued and safe, to believe in themselves and to grow into the person they are called to be. *“Let your light shine before others”* (Matthew 5:16)

Introduction

Our e-safety policy has been written by the school, building on the Leeds e-Safety Policy and government guidance. It has been agreed by all staff and approved by governors. It can be found on the school website.

The e-Safety Policy relates to other policies including those for Computing, Chromebook Agreement, anti-bullying and child protection, as well as the Staff Protocol for Safe and Secure use of AI.

- The school has an e safety coordinator; Michaela McGuigan, who will work with Child Protection designated staff: Allie Hopkinson (Headteacher/DSL), Debbie Webb (Learning Mentor), Monette St Rose (SENDCo) and Ruby Hanif (Deputy Headteacher)

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Teaching and learning

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation (including the use of AI tools).

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils comply with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy, including AI tools.

Managing Internet Access

Information system security

- School Computing systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- The school has two separate servers: the admin (office) and curriculum (rest of school).
- The Headteacher is the only person to be able to access both networks from one computer.
- The school has a wireless network which links with the curriculum server.

Wireless Network

- The school's wireless network is secure. There are required passwords, firewall certificates and proxy settings for every device that wishes to connect to the school WiFi.
- As Staff and Pupils will log in via unique logins, usual internet security will apply and accounts can be traced.
- Staff are advised to be careful when accessing with personal equipment.
- It will be managed by the ICT subject leader / e-safety coordinator and Computing technicians.
- Any breaches of the SENSO Filtering service will result in a notification being emailed to the E-Safety co-ordinator. Serious breaches will result in an instant notification. The E-safety co-ordinator will log breaches on CPOMS.

E-mail

- Pupils may only use approved virtual e-mail accounts on the school system (hosted by Purple Mash VLE).
- Pupils must immediately tell a teacher if they receive an offensive e-mail or message.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher, **Allie Hopkinson**, and Computing subject leader, **Michaela McGuigan**, will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Pupils' forenames only will be used on the website or Facebook Page, especially in association with photographs.
- All parents / carers will need to give consent before their child(ren)s photographs or videos will appear on the website.

Social networking and personal publishing

- Next Gen, via SENSO, will block/filter access to social networking sites.
- Sites will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and as part of staff training on E-safety.

Monitoring and Filtering

Monitoring strategies used by the school and staff include:

- 1) Physically monitoring by staff watching the screens of users.
- 2) Network monitoring using log files of internet traffic and web access.
- 3) Individual device monitoring through software and third-party services.

The school has invested in an external Monitoring and Filtering (F+M) provider (Watchguard) through our Technical Support Service (NextGen). This service provides two functions:

- Firewall and network security. It will actively block content and sites that are deemed inappropriate for access in school.
- Monitoring of all in school devices and Home Learning devices and recording of incidents and violations of safe internet policies.

The Curriculum Coordinator will perform weekly reviews of incident violation logs and inappropriate behaviour and breaches of the AUP will be addressed in line with the School's Behaviour Policies. Furthermore, the Headteacher/DSL will perform regular reviews to evaluate trends and patterns.

The Headteacher/DSL and the Curriculum Coordinator will review the M+F provision annually with our Technical Support Provider.

In addition to the Watchguard filtering service, the school also uses a monitoring service called SENSO. This provides a further enhancement of M+F and is installed on all the Home Learning Devices that are provided by the school. This service provides keystroke monitoring and reports on an exhaustive list of search terms that are considered to be in breach of Safer Internet standards and the AUPs. SENSO is a powerful M+F tool which can identify violations from an individual user, allows remote viewing and access to devices and provides customised reports to enable rapid and efficient responses to safeguarding incidents and issues.

- The school will work with Next Gen and SENSO to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator, **Michaella McGuigan**, who will report it to SENSO and/or Next Gen.

Managing emerging technologies

- Emerging technologies will be examined in school under the advisement of Next Gen and the Computing coordinator for educational benefit and a risk assessment will be carried out before use in school is allowed.

- School will also liaise with the Family of Schools on the subject of managing emerging technologies.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be required to use a school phone where contact with pupils is required.
- Please also see the Mobile Phone Policy.

Chromebooks

- Pupils in KS2 will be issued with the loan of a Chromebook to take home and for their use in school, following parental permission and signature of the Chromebook Agreement.
- Internet access on the device is restricted to permitted sites only, as released by staff.
- Staff must be sure that any sites being released for access by children are suitable and any discovery or breaches of this should be reported immediately to the school leadership.
- All Chromebooks are enrolled with the SENSO Monitoring and Filtering client and can be monitored remotely for breaches of the AUP and Safe Internet use.
- Where 'chat' functions are included in a platform (e.g. Google Classroom) all communications may be monitored and/or disabled at the discretion of the class teacher, Curriculum Coordinator or Headteacher/DSL.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Burley St Matthias CE Primary School holds the legal right to collect and use personal data relating to pupils and their families, and we may also receive information regarding them from their previous school, LA and/or the DfE. We collect and use personal data in order to meet legal requirements and legitimate interests set out in the GDPR and UK law, including those in relation to the following:

- o Article 6 and Article 9 of the GDPR
- o Education Act 1996
- o Section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013

In accordance with the above, the personal data of pupils and their families is collected and used for the following reasons:

- o To support pupil learning.
- o To monitor and report on pupil progress
- o To provide appropriate pastoral care, including safeguarding
- o To communicate information about any of the above points
- o To communicate information about the business of the school
- o To assess the quality of our service
- o To comply with the law regarding data sharing

<https://www.burleystmatthias.co.uk/leeds/primary/burleystmatthias/arenas/websitecontentcommunity/web/bsmgdprprivacynoticepupilsandtheirfamilies.pdf>

Policy Decisions

Authorising Internet access

- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Leeds City Council can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit Computing provision to establish if the e-safety policy is adequate and that its implementation is effective.
- The School also recognises it has a role in preventing radicalisation of students from a range of sources. It therefore has a due regard for the need to prevent people being drawn into any form of terrorism and has subscribed to the guidance given in 'Prevent: Radicalisation and Extremism: Prevent Duty Guidance for specified authorities in England and Wales on the duty in the Counter-Terrorism and Security Act 2015'.

<https://www.gov.uk/government/publications/prevent-duty-guidance/revised-prevent-duty-guidance-for-england-and-wales>

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the e-safety co coordinator **Michaela McGuigan** and a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher **Allie Hopkinson**.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Cyberbullying

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- All procedures to investigate incidents or allegations of Cyberbullying will be in accordance with the schools anti-bullying policy.
- Where crimes may have been committed online, these will be reported to the police.

Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year. Pupils will be informed that network and Internet use will be monitored.
- Pupils will be taught using Twinkl and CEOP lesson plans and resources.

www.thinkuknow.co.uk

Staff and the e-Safety policy

- All staff will be given access to the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

The Policy was shared with staff and governors.

Thereafter it will be reviewed **regularly** as part of the school's cycle of reviewing policies.

Appendix 1: Acceptable Use Policy for Pupils

When using the school's ICT equipment and other information systems, I have understood and will comply with the following statements

- I have read and know what the computer rules in this document mean to me.
- I will only go on the internet using my own username and password.
- I will make sure that my password for the internet is difficult to guess and I will not share my password with anybody else.
- If I think someone has guessed my password I will tell a teacher.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I see anything like this I will tell my teacher immediately.
- I will not try and get to any websites that the school has blocked access to.
- I will make sure I take care of any school-owned ICT equipment that I use in school or at home.
- I will only use memory sticks with permission from my teacher.
- I will not install any software on school computers.
- I will return any school-owned ICT equipment to (name of person) when I have finished using it.
- I know that my use of ICT can be checked and that my parent/carers will be contacted if a member of school staff is concerned about my safety or conduct.
- I will not damage any school-owned ICT equipment.
- I will not eat or drink while using school-owned ICT equipment.

Social Media

- I know that some websites and social networks have age restrictions and I should not use them unless I am old enough.
- I will not say nasty or hurtful things about any member of staff or pupil online.
- I will not give away any of my personal details (full name, age, date of birth, sex, address etc.) or the personal details of other users in school, over the internet. This includes photographs or video images of me, other pupils or members of staff.
- I will never arrange to meet anyone I have only met online unless a trusted adult is with me.
- If I see any hurtful comments about the school, staff or pupils. I will take screenshots for evidence and report to the eSafeguarding coordinator. (Mrs Hopkinson)
- Where 'chat' functions are included in a platform (e.g. Google Classroom) all communications may be monitored and/or disabled at the discretion of the class teacher, Curriculum Coordinator or Headteacher/DSL.

Managing Digital Content

- I will only use school-owned equipment to create pictures, video and sound. Pictures, video and sound will not be taken without asking permission first.
- I will not publish anything online, e.g. images or pictures, without asking my teacher.

Email

- I will only use my school email address to contact people I know or those agreed by my teacher.
- I will take care in opening any attachments sent by email. I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- When sending emails I will make sure that they are polite and sensible. I will not use my school email account to forward chain emails.

Mobile phones and devices

- I will only bring my mobile phone or other devices to school with permission from my teacher.
- I will only use mobile phones and mobile devices (e.g. Nintendo DS) when my teacher tells me I can.
- I will not take pictures in school on my mobile phone or mobile device.

AI

- **Data privacy:** I will not enter any personal, confidential, or sensitive information into AI tools, as this information may be stored and shared online.
- **School-approved use:** I will only use AI when specifically allowed by a teacher and for educational purposes that have been approved in advance.
- **No AI for cheating:** I will not use AI to generate complete assignments to present as my own work, and will be aware of the difference between using AI as a tool and using it to cheat.
- **Attribution:** When using AI for schoolwork, I will properly attribute any AI-generated content.
- **Understand AI's limitations:** I am aware that AI can be inaccurate or make errors ("hallucinations") and should not be relied upon for factual information, especially concerning personal health or well-being.
- **Age restrictions:** I will follow the minimum age requirements for AI tools, as some are restricted to users 13 or 18 and over.
- **School monitoring:** I understand that the school may monitor my use of its IT systems and devices.

Agreement

I agree to follow the rules set out in this AUP. I know that if I break any of these rules my parent/carers may be told and my school internet account may be suspended.

Pupil name

Signed

Parents Signature

Date

Please see over for more information on Parental Controls

Parental Controls

The online world gives us access to a huge amount of information and services, but the scale of information available also means that there is content that is inappropriate for children. What is or isn't appropriate is up to individual parents to decide, and could be based on things like age, ability, beliefs and family views.

Parental controls allow you to block and filter upsetting or inappropriate content. They work across your WiFi, phone network, individual apps and devices.

Parental controls can help you:

- Plan what time of day your child can go online and how long for.
- Create content filters to block apps that may have inappropriate content.
- Manage the content different family members can see.

For further information about how to set up parental controls on:

- Home broadband and WiFi
- Games consoles
- Mobiles, tablets and computers
- Apps and online services
- Search engines
- WiFi and being away from home

Visit <https://nspcc.org.uk/keeping-children-safe/online-safety/parental-controls/>

Appendix 2: Staff Acceptable Use Policy



Staff ICT Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites.
- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system). I will not share my username or password with anyone else.
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no

longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used for the purposes of the curriculum or school marketing and will always consider parental consent. Any images to be shared outside of the safe school community will be first approved by the Head Teacher.

- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. I will not connect any personal devices to the school network without first checking for up to date anti-virus software with the ICT technicians (NextGen). Where possible I will use the School Learning Platform to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.
- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
- I will respect copyright and intellectual property rights.
- I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.
- I will report all incidents of concern regarding children's online safety to the Designated Child Protection Officer (Allie Hopkinson, Debbie Webb, Ruby Hanif or Monette St Rose) and/or the e-Safety Coordinator as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the e-Safety Coordinator or the designated lead for filtering as soon as possible.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. I will not attempt to access the internet via any ISP other than ICT4 Leeds whilst on school premises. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT Support Provider/Team as soon as possible.
- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Emails between pupils and staff must take place using a specifically allocated Purple Mash or Google Classroom account allocated by the ICT coordinator, Michaela McGuigan and not via staff email accounts. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.
- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the Council, into disrepute.

- I will only use AI for Enhancing Productivity: I will utilise AI tools for tasks such as drafting internal guidance and documents, creating lesson plans, conducting research, summarising content and generating ideas. I will always review AI-generated content for accuracy, appropriateness and relevance. AI will support, as scaffolding, my content and not be a direct replacement. AI will support, not replace, my professional judgement. When using AI, particularly in communications or content creation, I will be transparent about its use, ensuring that all stakeholders understand how AI has contributed to the work. I must ensure all data used within AI Tools is anonymised where possible and complies with UK GDPR. I will not use AI for generating content that may be misleading, biased, inappropriate or unethical. I will ensure AI-generated work reflects the values and standards of Burley St. Matthias. I will be aware that AI tools can produce inaccurate or biased content. I will always cross-check AI outputs against reliable sources and professional expertise.
- I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the e-Safety Coordinator or the Head Teacher.
- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy.

Signed: Print Name: Date:

Accepted by: Print Name:

Appendix 3: Pupil Chromebook Loan Agreement



Name of pupil: _____ Year: _____

Device ID: _____

1) This agreement is between:

- i) Burley St Matthias CE Primary School ("the school")
- ii) Name of parent _____ ("the parent" and "I")
Address: _____

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 devices 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.

- 1. The school is lending the pupil a Chromebook ("the equipment") for the purpose of doing schoolwork at school and from home on work or special projects, etc.
- 2. This agreement sets the conditions for taking a Burley St Matthias CE Primary School Chromebook ("the equipment") home.

I confirm that I have read the terms and conditions set out tin 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 when it is not on school property.

If the equipment is damaged, lost or stolen, I will immediately inform the school business manager, and I acknowledge that I am responsible for the reasonable costs requested by the school to repair or replace the equipment (costs not exceeding £50.00 per device). 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 the demand from the school, in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

If the equipment is damaged, lost or stolen, and your child is eligible for the pupil premium, contact the school business manager.

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 or siblings
- Don't leave the equipment unsupervised in unsecured areas

3) Unacceptable use

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

Where 'chat' functions are included in a platform (e.g. Google Classroom) all communications may be monitored and/or disabled at the discretion of the class teacher, Curriculum Coordinator or Headteacher/DSL.

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
- Allowing other persons to access or create any inappropriate content as above

I accept that the school will sanction the pupil, in line with the school 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:

- Make sure my child locks the equipment if it is left inactive for a period of time
- Do not share the equipment between friends or family
- If the device prompts me for the systems update, return the device to school for this to be installed.

If I need help doing any of the above, I will contact the School Business Manager on the school office email:

office@burleystmatthias.co.uk

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 school if the pupil no longer attends the school.

7) Parental responsibilities

- to ensure that your child adheres to the signed agreement

8) 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	
Date	

Original document to be kept in school and a copy to be returned to parent

Parental Controls

The online world gives us access to a huge amount of information and services, but the scale of information available also means that there is content that is inappropriate for children. What is or isn't appropriate is up to individual parents to decide, and could be based on things like age, ability, beliefs and family views.

Parental controls allow you to block and filter upsetting or inappropriate content. They work across your WiFi, phone network, individual apps and devices.

Parental controls can help you:

- Plan what time of day your child can go online and how long for.
- Create content filters to block apps that may have inappropriate content.
- Manage the content different family members can see.

For further information about how to set up parental controls on:

- Home broadband and WiFi
- Games consoles
- Mobiles, tablets and computers
- Apps and online services
- Search engines
- WiFi and being away from home

Visit <https://nspcc.org.uk/keeping-children-safe/online-safety/parental-controls/>