Balderstone St Leonard's C Of E Primary School.

Online Safety Policy Updated August 2023

This Online Safety policy was approved by the Governing Body / online safety governor Jonathan Greenwood on:	September 2023

The implementation of this Online Safety Policy will be monitored by the:	Headteacher, Senior Leadership Team, Chair of Governors
Monitoring of the policy will take place at regular intervals:	Termly at full governors
The Governing Body will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	At Least termly within the Safeguarding section of the Headteachers' Report to Governors
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments (changes/additions to KCSIE 2023) in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2024
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LA Safeguarding Officer, LADO, Police

Balderstone monitors and reviews the effectiveness of this policy through:

- Use of CPOMS to manage and logs of child-on-child abuse/cyberbullying/inappropriate use of technology
- Monitoring logs of internet activity (including visited sites/using Netsweeper Digital Services) to monitor network activity
- Drop-in/spot checks of internet history, folders and files
- Surveys and questionnaires – children, parents and staff

Scope of this policy

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

Keeping Children Safe in Education 2023 states that it is essential that children are safeguarded from potentially harmful and inappropriate online material. Our effective whole school approach to online safety empowers our school to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk that we educate staff, parents and pupils in:

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

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

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

commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If our pupils or staff are at risk, this would be reported to the Anti-Phishing Working Group (https://apwg.org/).

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 cyberbullying or other Online Safety incidents covered by this policy, which may take place outside of the school (with parent and school owned Ipad use), but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy/acceptable usage policy.

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

Aims of this policy

In an increasingly digital/online world we aim that our children are digitally literate, whilst wise to both the pitfalls and benefits that technology brings. At Balderstone we aim:

- To allow children to maximise the benefits and opportunities that technology has to offer. Offer 1:1 devices in KS2 to increase digital literacy, knowledge and expertise.
- To ensure appropriate security is in place that is balanced with the need to learn effectively.
- To ensure children are equipped with the skills and knowledge to learn effectively.
- To teach children about the risks associated with technology and how to deal with them both within and outside the school environment.
- To keep up to date with the latest Online Safety information and safeguarding information in line with Keeping CHildren Safe in Education 2023.
- To ensure children feel confident to talk about their online world and issues that affect them.
- To ensure that children know what to do if faced with online content that is inappropriate and needs reporting.
- To care for all our learners, especially our most vulnerable learners ensuring they use technology wisely and safely without exploitation.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within Balderstone school:

Governors

Governing bodies should ensure online safety is an ongoing and interrelated theme whilst devising and implementing their whole school approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement. Governors are responsible for the approval of the Online Safety Policy and for strategically reviewing the effectiveness of this policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body (Jonathan Greenwood) has taken on the role of Safeguarding Governor. The role of the Safeguarding/ Online Safety Governor may include:

- regular meetings with the Designated Safeguarding Lead/DSL
- regular monitoring of online safety incident logs/ CPOMS logs
- regular monitoring of filtering
- reporting to relevant Governors committees (Church, curriculum and Community committee)

Headteacher and Senior Leaders

- The Headteacher (as lead Designated safeguard lead) has a duty of care for ensuring the safety (including Online Safety) of members of the school community The day-to-day responsibility for online safety will be held by the Designated Safeguarding Lead, supported by the Deputy Safeguarding Lead (Mrs Draycott)

- The Headteacher and (at least) another member of the Senior Leadership should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

- The Headteacher and Senior Leaders are responsible for ensuring that the Designated Safeguarding Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- The Senior Leadership Team will receive regular monitoring reports from the Designated safeguarding Lead via Senior Leadership Meetings.

Designated Safeguarding Leaders

The designated safeguarding lead (Mrs Gow) will take **lead responsibility** for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This is explicit in Designated Safeguarding Lead's job description.

- liaise with staff (especially teachers, pastoral support staff, school nurses, IT technicians, senior mental health leads and special educational needs co- ordinators (SENCO's), or the named person with oversight for SEND in a college and senior mental health leads) on matters of safety and safeguarding and welfare (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies so that children's needs are considered holistically
- are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college
- can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online
- As part of our school commitment to safer recruitment Mrs Johnstone as our School business manager will inform any shortlisted candidates for any school vacancies/volunteer roles that online searches will be carried out.
- The DSL takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents at least annually.

- The DSL ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.

- The DSL (with support from Computing lead) provides/signposts training and advice for staff. **All** staff should receive appropriate safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring at induction and in safeguarding training updates annually.

- The DSL liaises with the Local Authority.

- The DSL liaises with school technical staff MCC Digital services and BT Digital services

- The DSL receives reports of online safety incidents (Via CPOMS) and creates a log of incidents to inform future online safety developments.

- The DSL ensures that the school network/ internet/ email is regularly monitored in order that any misuse or attempted misuse can be reported to Designated Senior Leaders; LADO/police for investigation/ action/ sanction.

- The DSL meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs.

- The DSL attends relevant meetings / committee of Governors.

- The DSL reports regularly to Senior Leadership Team regarding online safeguarding .

- The school's DSL should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:
    - sharing of personal data
    - access to illegal / inappropriate materials
    - sexual abuse online
    - inappropriate on-line contact with adults / strangers
    - potential or actual incidents of grooming
    - online-bullying

Technical staff

The Technical Staff/ MCC Digital services and Digital services team are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- the filtering policy is applied and updated on a regular basis.
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- that the use of the network/ internet/ email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher; Designated Safeguarding Lead; Designated Senior Leader; LADO for investigation/ action/ sanction.
- that monitoring software/ systems are implemented and updated as agreed in school policies.

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices. They attend and understand the training delivered in school/online on online safety AND ask about anything they are unsure of.
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (SAUP).
- they report any suspected misuse or problem to the Headteacher; Designated Safeguarding Lead; LADO for investigation / action / sanction.
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems and school email address.
- online safety issues are embedded in all aspects of the curriculum and other activities.
- pupils understand and follow the Online Safety Policy and acceptable use policies.
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. Where possible websites and search engine results are checked and monitored prior to lesson delivery. Swiggle is the search engine of choice in school.

- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

It is essential that all our Balderstone staff receive online safety training and understand their responsibilities, as outlined in this policy.

Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- The Designated Safeguarding Lead will receive regular updates through attendance at external training events (eg relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings/ INSET days.
- The Designated Safeguarding Lead will provide advice/ guidance/ training to individuals as required.

Pupils

- Pupils are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement (PAUA)
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Pupils need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Pupils will be expected to know and understand policies on the use of mobile devices, Ipads and digital cameras. They should also know and understand policies on the taking / use of images, consent and online-bullying.
- Pupils should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in our school family, ensuring that their children understand the need to use the internet/ mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' meetings, use of Jamf parent app, newsletters, letters,

website and information about local or national online safety campaigns or information. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events (no social media posting of photos/videos that include images of other children/staff)
- their children's personal devices in the school (where this is allowed). This is covered in our Mobile Communications Policy.

Community/visitor Usage

Community Users/visitors who access school systems / website as part of the wider school provision will be expected to sign a (Community User AUA) before being provided with access to school systems/network. Passwords must NOT be saved or 'keychained' on personal devices.

Education and Online Safety

It is our school aim to provide a balanced and relevant approach to the use of new technologies. We maintain a sensible approach to balancing the management of risks/benefits with technology, encouraging the children to be proactive in making wise online choices. The education of pupils in online safety/ digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. Balderstone uses a three-fold approach to digital safety education:

1. use of well-structured sequence of lessons from Project Evolve to highlight the importance of safely preparing for a digital world
2. use of PSHE, worship and Computing lessons to teach the importance of respect, consent and wisdom.
3. Online safety will be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. Our online safety curriculum is broad, relevant and provides progression:

- Our planned online safety curriculum is provided as part of Computing and PHSE/ RSE lessons and should be regularly revisited.
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in wise decision-making.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. This can be done via Showbie or Swiggle on the iPads.
- Pupils in school are NOT freely allowed to search the internet randomly, but there may be occasions in KS2 where pupils are researching a topic/theme. Staff should be vigilant in monitoring the content of the websites the young people visit and discuss what to do if they come across something inappropriate.

- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination or use of You tube etc) that would normally result in internet searches being blocked. In such a situation, staff can request that the DSL (or other relevant designated person from MCC) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Parents / Carer engagement

Some parents and carers may have a limited understanding of online safety risks and issues, yet they play an essential role in the education of our/their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Balderstone St Leonard's seeks to provide information and awareness to parents and carers through:

- Curriculum activities/Twitter feeds
- Support from the safeguarding governor (online safety)
- Tutorials on how to use parent safe apps such as Jamf parent
- Letters, newsletters, web site, Learning Platform
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

Technical information– infrastructure / equipment, filtering and monitoring

As highlighted in the 2023 Keeping Children Safe in Education statutory guidance, filtering and monitoring is of paramount importance:

Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and DSLs should be doing all that they reasonably can to limit children's exposure to the online risks from the school's IT system. As part of this process, our governing body ensures that Balderstone has appropriate filtering and monitoring systems in place and regularly reviews their effectiveness. The governors ensure that the computing leadership team (Mrs Gow , Mrs Draycott and Mrs Turner) and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. As a school we consider the number of and age range of our children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.

"Schools in England (and Wales) are required "*to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering*"[1]. Furthermore, the Department for Education's statutory guidance 'Keeping Children Safe in Education' [2] obliges schools and colleges in England to "*ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to the above risks*[3] *from the school's or college's IT system*" however, schools will need to "*be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding*." UK Safer Internet Centre

The appropriateness of our filtering and monitoring systems are sufficient and provided by Lancashire Digital Services (Netsweeper) required by the Prevent Duty.

Our filtering and monitoring procedures:

- Mrs Gow (with support from BTLS Digital services and MCC) manages the filtering and monitoring systems.
- Mrs Gow reviews the filtering and monitoring provision at least annually.
- Filtering system is checked on a weekly basis to ensure that we block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet their safeguarding needs

The school, with DSL leadership will be responsible for ensuring that the school infrastructure and network is as safe and secure as is **reasonably** possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities.

- Technical systems will be managed in ways that ensure that the school meets recommended technical requirements (school is now on Gigafast broadband)
- There will be regular reviews and audits of the safety and security of school technical systems – **weekly** monitoring reports are generated on online use, suspicious searches, Prevent related searches and delivered to DSL.
- Servers (in school library and office), wireless systems and cabling is securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS2) will be provided with a username and secure password for 1:1 device and own school Microsoft outlook email address.
- Users are responsible for the security of their username and password.
- The "master / administrator" passwords for the school's ICT systems, used by the Network Manager (or other person) must also be available to the Headteacher and Designated Safeguarding Lead and kept in a secure place (eg school safe)
- MCC Digital Systems are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing and filtering search is conducted weekly on staff devices (on rota) and on selected children's devices. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes through the Helpdesk.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided differentiated user-level filtering
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the

security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

- Clear information is provided to users of temporary access e.g. “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.

- If appropriate, an agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.

- No removable media devices other than school provided encrypted USB memory sticks are used unless these are approved by the headteacher and are in line with policies including GDPR etc. **Personal/sensitive data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured**.

Use Of Mobile Devices

Mobile phones

Children are **not** allowed to bring mobile phones into school. The only exception is for children with diabetes/medical conditions that use mobile data monitoring.

If a mobile phone is brought into school by a child, staff will remove it from the child and keep it safe until the end of the day. Parents/carers will be informed and asked to collect the mobile phone from class teacher or to meet with Mrs Gow if this is a recurring incident.

Staff may bring mobile phones into school for personal use but these must be switched off during teaching sessions. (they may only be switched on in exceptional circumstances, e.g an emergency). If a member of staff needs to have their phone on during the day, they must inform the Headteacher.

Mobile phones should NEVER be used in classrooms with children present without express permission from the headteacher. The staffroom, office and Mrs Gow's office are all areas where (as long as no pupils are present) phones may be accessed. The office will monitor phones for staff if any staff member is expecting an urgent communication.

Staff may use their mobile phones in the staff room/office or anywhere in the building once all children have left the building at the end of the day.

Staff may carry their own mobile phones when taking children off site on educational visits. This is for emergency contact and staff should use the Call Switch Communicator app to log calls (to prevent parents/carers storing staff numbers)

Staff must not use their personal phones to take pictures, videos or make recordings of children.

Staff phones should NOT be used on the school's internet/logged on to the school network at any time.

Other Mobile Devices

School cannot be held liable for damage to or the loss of any mobile device brought into school.

Use Of Digital Media (cameras and recording devices)

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/ carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying/misuse and harassment to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and

educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites. Pupils are taught about the importance of consent for digital images.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press. This will be done through the schools Home School Agreement.

- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy, and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *pupils* in the digital / video images. The school can ban taking of photos in particular circumstances, eg where there are children in a performance who do not have photo permissions/not appropriate for digital images to be taken.

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on **school equipment**, the personal equipment of staff should **not** be used for such purposes.

- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Pupils must not take, use, share, publish or distribute images of others without their permission. Photographs of children are not to be Airdropped between pupils unless for educational purposes.

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Pupil's work can only be published with the permission of the parents or carers (signalled on home/school agreement)

Photographs of children and school events can be taken by any member of staff who should only use school equipment.

When taking photographs staff should respect the consent, dignity and rights of the individuals.

Staff are responsible for ensuring images are stored responsibly and that they are deleted once they are no longer needed taking regard to retention policies and GDPR regulations.

The class IPAD must be passcode protected and only the class teacher should access it.

Photographs held on the IPAD must be used and deleted as soon as possible.

Photographs that are being stored for curriculum evidence should only be on the class teachers lap top. These may be kept until the end of the academic year in which they are taken.

The class teachers Macbook air/laptop must be password/fingerprint protected.

It is recognised that teachers may need to work with photographs at home.
Photographs should only ever be stored on a school password protected device.

PHOTOGRAPHS OF CHILDREN MUST NEVER BE DOWNLOADED ONTO DEVICES OR PCS THAT ARE NOT SCHOOL OWNED.

Publication Of Images.

Consent is gained from parents for publication of images.

When images are published care is taken to ensure that individual children and adults cannot be identified. No personal information accompanies published images.

Staff must ensure that when using social networking personal profiles are secured and that they do not display content that is detrimental to their own professional status or that could bring the school into disrepute. (see staff code of conduct)

CCTV, video conferencing, VOIP and Webcams

Parents will be informed if CCTV, video conferencing or webcams are to be used in school.

All video conferencing sessions will be logged outside of remote teaching sessions.

Communication Technologies

When using communication technologies, the school considers the following as good practice:

- The official school email service (Microsoft 365 email address @balderstone.lancs.sch.uk) may be regarded as safe and secure and is monitored. **Users should be aware that email communications are monitored.** Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems.

- Users must immediately report, to the class teacher and then the DSL– in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and pupils or parents/ carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems.

- **Personal email addresses, text messaging or social media must not be used for these communications.**

- Whole class email addresses may be used at KS1, while students / pupils at KS2 and above are provided with individual school email addresses for educational use.

- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need

- to communicate appropriately when using digital technologies.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

- Each class has an email account on the Office 365 system.
- All email may be monitored at any time in accordance with the acceptable use policy.
- School governors should use their school associated, named account to communicate school business and the official Governor Whatsapp can be used to alert governors to check official emails.
- Staff official Whatsapp group can be used for admin, messages, wellbeing information and shared news, greetings and informal work messages. However, pupils should not be identified other than by initials (year groups) in these messages.
- Staff should use their out-of-hours messages and scheduled send options to help with their wellbeing and work/life balance.

Social networks.

The use of social networking sites such as Facebook, Bebo, Snapchat, TikTok Twitter and MySpace is common for communication between friends and family. In addition there are many sites which allow people to publish their own pictures, text and videos such as You Tube and Instagram.

Careful use of these sites should have no impact on the professional role of staff in school.

However, use of these sites does not provide a completely private platform for personal communication.

To protect themselves, staff should follow the guidance below:

Staff must not access these sites for personal use during working hours.

Content on Social Network sites may be unmediated and inappropriate for certain audiences. Staff must ensure that their privacy settings are appropriate and proportionate to allow them to follow the professional code of conduct.

If a Social Network site is used personally, details must not be shared with children and privacy settings should be reviewed regularly to ensure information is not shared with a wider audience than intended. Content posted online must not :-

- Bring the school into disrepute
- Lead to valid parental complaints
- Be deemed derogatory towards the school and/or its employees.
- Be deemed derogatory towards pupils and/or parents and carers.
- Bring into question their appropriateness to work with children or young people.

Adults must not communicate with children using any digital technology where the content of the communication may be considered inappropriate or misinterpreted.

Staff should not communicate online with parents, past pupils or siblings of pupils. An exception is email communication with parents from school email addresses.

Children or parents must not be added as “friends” on any social networking site.

The school will not access social networking sites to ‘vet’ prospective employees.

Instant Messaging

Staff must not use school equipment to communicate with personal contacts.

School Website

There is a dedicated Online Safety section on the school website under the Curriculum area of computing.

The website content is managed by the Headteacher.

All staff who have access to edit the website are aware of Online considerations.

All downloadable materials must be uploaded in PDF format.

Infrastructure And Technology

Children’s can access the school system within lessons. The school system is filtered and security protected. BTLS filtering.

Children have access to their own file on the curriculum server in which to store their work and on Showbie.

Staff access to school systems is restricted according to areas of responsibility.

All users of the school network have a secure user name and password.

An update register of all hardware is kept.

An up to date record of all licenses for software is kept.

Software is installed by the school technician.

Dealing With Incidents

Any suspected illegal material or activity must be brought immediately to the attention of the Headteacher'DSL who has to refer this to the external authorities.

Never personally investigate, interfere with or share evidence as you may be inadvertently committing an illegal offence.

Inappropriate Use & safeguarding

DFE Safeguarding guidance states:

- All staff should sign an Acceptable Use policy (AUP) before using the school network.
- The online Safety policy is reviewed on an annual basis.
- Adults should ensure that pupils are never listed as approved contacts on any social networking site.
- Adults should never access the social networking sites of pupils.
- Adults should never give personal contact details to pupils, including their mobile phone number.
- Adults should only make contact with children for professional reasons.
- Adults should not use the internet or web-based communication channels to send messages to a child

Disciplinary action may be taken in relation to those members of staff who choose not to follow the advice and guidance outlined in this policy.

Any inappropriate use should be reported to the Headteacher/DSL.

A log of any inappropriate use will be kept and monitored by the Headteacher.

All staff and children sign an acceptable use policy (AUP).

Monitoring & Reporting Misuse

Updated in line with Keeping Children Safe in Education 2023. Children will be regularly reminded that they must speak out if they notice anything online that causes concern.

Monitoring Logs of any concerning network use are emailed to the Headteacher weekly. All staff are trained to manage a report. Effective safeguarding practice includes:

- if possible, managing reports/online abuse/images with two members of staff present, (preferably one of them being the designated safeguarding lead or a deputy)
- careful management and handling of reports that include an online element. Including being aware of searching screening and confiscation advice (for schools) and UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people. **The key consideration is for staff not to view or forward illegal images of a child.** The highlighted advice provides more details on what to do when viewing an image is unavoidable. In some cases, it may be more appropriate to confiscate any devices to preserve any evidence and hand them to the police for inspection
- Staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online, this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non- consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content. Staff should follow the usual safeguarding and reporting policy.

Children should never have completely unsupervised use of the internet in school. Class teachers and other staff members should be within sight and sound of children using technology.

The opportunities for children to access the internet should be planned and closely monitored.

Children should never be allowed to use search engines randomly. Swiggle is the school's preferred child safe search engine.

Safeguarding Issues

Online safeguarding is part of overall safeguarding culture in our school

The designated lead for safeguarding (DSL) is Mrs Gow

The back-up DSL is Mrs Draycott

Mrs Gow has in-depth annual training in online safeguarding.

All staff have annual updates in online safeguarding

Jonathan Greenwood is the online safety governor. He carries out an annual audit of online safety in school and reports to governors.

Any Issue relating to online safety is reported to the DSL and is dealt with as any other safeguarding issue.

Out of school incidents brought to a member of staff's attention are also dealt with in line with the school safeguarding policy. School has adult of care to the children.

Parents are regularly encouraged to engage with online safety issues, through the school newsletter and the website.

The school always observes Safer Internet Day and online safety is a continuing part of the curriculum.

Children know they can talk to a trusted adult about online safety.

Online abuse protocol

- Secure the device
- Switch it off / blank the screen
- Seek advice from DSL
- The DSL will seek further advice if needed
- Consider the best interests of the child – the frequency, extent, extremity of the incident
- DSL will record as a safeguarding incident with actions recorded and followed up

Communicating with both current and former pupils via social networking sites or via other non-school related mechanisms such as personal e-mails and text messaging can lead to employees being vulnerable to serious allegations concerning the safeguarding of children and young people.

All staff should are aware that children can abuse other children at any age (often referred to as child-on-child abuse). And that it can happen both inside and outside of school **and online**. It is important that all staff recognise the indicators and signs of abuse and know how to identify it and respond to reports.

All staff should be clear as to the school policy and procedures with regards to child-on-child abuse (see anti-bullying/child-on-child abuse policy). Child-on-child abuse is most likely to include, but may not be limited to:

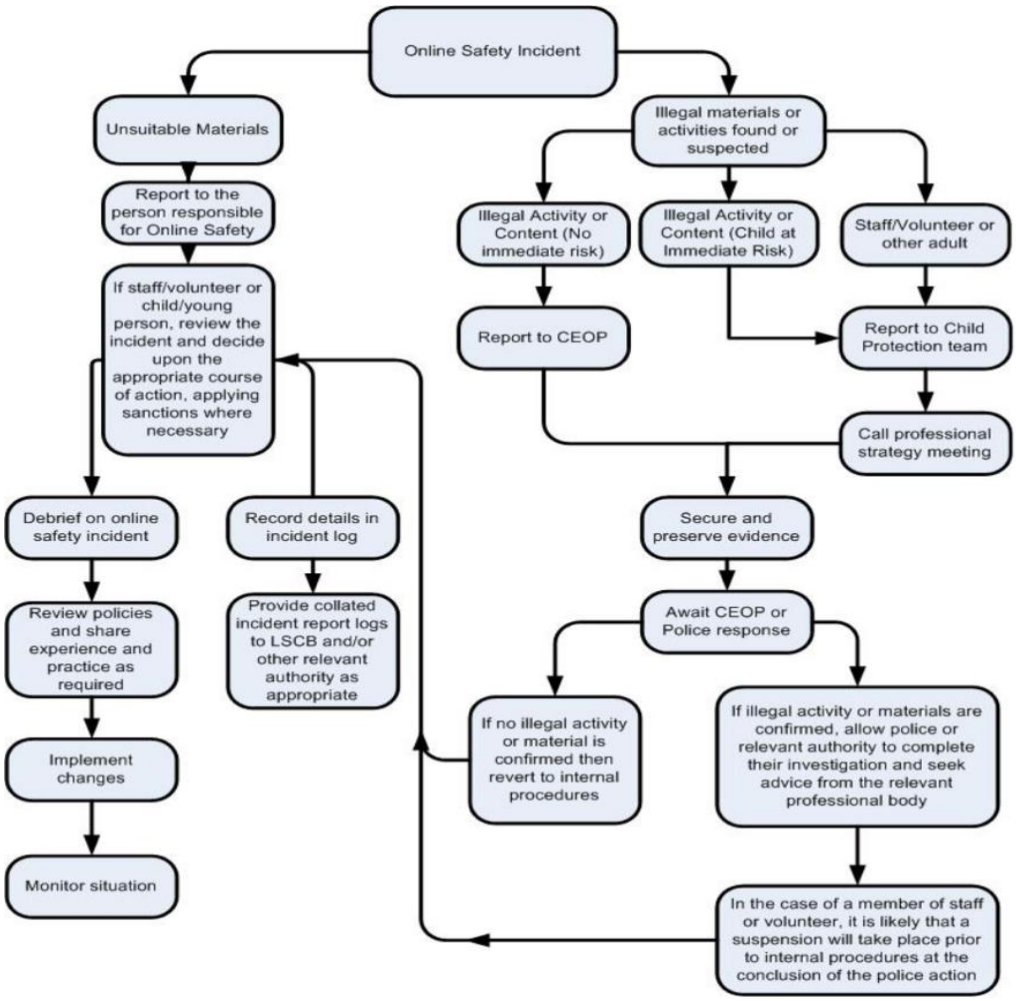
- bullying (including **cyberbullying**, prejudice-based and discriminatory bullying)
- sexual harassment, such as sexual comments, remarks, jokes and **online** sexual harassment

County lines Children are also increasingly being targeted and recruited online using **social media**.

Harmful sexualised behaviour can occur online and/or face-to-face and can also occur simultaneously. Abuse that occurs online or outside of the school should not be downplayed and should be treated equally seriously following the safeguarding and child protection policy guidelines.

Abuse can take place wholly online, or technology may be used to facilitate offline abuse.

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



In the event of suspicion of a safeguarding concern, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures
- Involvement by Local Authority / Academy Group or national / local organisation (as relevant). o Police involvement and/or action

If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

School Actions & Sanctions

It is likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Actions / Sanctions linked to Balderstone Behaviour policy

Pupil Incidents/Sanctions	Refer to class teacher	Refer to Deputy Head	Refer to Headteacher / DSL	Refer to Police	Refer to technical support staff for action r.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention /suspension
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X		X			X
Unauthorised use of non-educational sites during lessons/wasting learning time	X	X				X			

Unauthorised / inappropriate use of mobile phone /digital camera / other mobile device	X		X			X			
Unauthorised / inappropriate use of social media /messaging apps / personal email	X		X			X			
Unauthorised downloading or uploading of files (appropriate content)	X		X			X			
Allowing others to access school network by sharing username and passwords	X		X		X	X	X		
Attempting to access or accessing the school / network, using another student's / pupil's account/passwords	X		X		X	X	X	X	X
Attempting to access or accessing the school / academy network, using the account of a member of staff	X		X		X	X	X	X	X
Corrupting or destroying the data/documents of other users	X		X		X	X	X	X	X
	X		X			X	X	X	X

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature									
Continued infringements of the above, following previous warnings or sanctions	X		X			X	X		X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school	X		X			X		X	X
Using proxy sites or other means to subvert the school's / academy's filtering system	X		X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X		X			X			
Deliberately accessing or trying to access offensive or pornographic material	X		X			X	X	X	X
Receipt or transmission of material that infringes the									

copyright of another person or infringes the Data Protection Act			X		X	X	X	X	X

Actions / Sanctions

Staff Online Code of Conduct	Refer to senior leader	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X		X	X	X
Inappropriate personal use of the internet / social media /personal email		X	X			X	X	X
Unauthorised downloading or uploading of files		X	X			X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X	X			X		

Careless use of personal data e.g. holding or transferring data in an insecure manner/non-GDPR compliance		X	X			X		X
Deliberate actions to breach data protection or network security rules		X	X		X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X		X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X	X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out unsolicited digital communications with pupils		X	X		X	X	X	X
Actions which could compromise the staff professional standing (against code of conduct)		X	X		X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X		X	X	X	X

Using proxy sites or other means to subvert the school's / filtering system		X	X		X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X		X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X	X	X	X
Breaching copyright or licensing regulations		X	X		X	X	X	X
Continued infringements of the above, following previous warnings or sanctions		X	X		X	X	X	X

Appendices

Useful contacts and websites used for staff training, parental workshops and remote learning.

- **National Crime Agency's CEOP Safety Centre:** The CEOP Safety Centre aims to keep children and young people safe from online sexual abuse. Online sexual abuse can be reported on their website and a report made to one of its Child Protection Advisors.
- **Online:** Schools and colleges should recognise that sexual violence and sexual harassment occurring online (either in isolation or in connection with face-to-face incidents) can introduce a number of complex factors. Amongst other things, this can include widespread abuse or harm across a number of social media platforms that leads to repeat victimisation. Online concerns can be especially complicated and support is available from:
    - **The UK Safer Internet Centre** provides an online safety helpline for professionals at 0344 381 4772 and helpline@saferinternet.org.uk. The helpline provides expert advice and support for school and college staff with regard to online safety issues

- **Internet Watch Foundation**: If the incident/report involves sexual images or videos that have been made and circulated online, the victim can be supported to get the images removed by the Internet Watch Foundation (IWF)
- **Childline/IWF** *Report Remove* is a free tool that allows children to report nude or sexual images and/or videos of themselves that they think might have been shared online

- **UKCIS Sharing nudes and semi-nudes advice**: Advice for education settings working with children and young people on responding to reports of children sharing non-consensual nude and semi-nude images and/or videos (also known as sexting and youth produced sexual imagery). Please see footnote 8 for further information
- National Crime Agency's CEOP Education Programme provides information for the children's workforce and parents and carers on protecting children and young people from online child sexual abuse.
- LGFL 'Undressed' provided schools advice about how to teach young children about being tricked into getting undressed online in a fun way without scaring them or explaining the motives of sex offenders.

Online safety-advice

Childnet provide guidance for schools on cyberbullying
Educateagainsthate provides practical advice and support on protecting children from

extremism and radicalisation

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

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

Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective

Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones

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

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

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

Online safety guidance if you own or manage an online platform DCMS advice A business guide for protecting children on your online platform DCMS advice

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

Online Safety- Support for children

Childline for free and confidential advice
UK Safer Internet Centre to report and remove harmful online content CEOP for advice on making a report about online abuse

Online safety- Parental support

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

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

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

Internet Matters provide age-specific online safety checklists, guides on how to set parental controls, and practical tips to help children get the most out of their digital world

How Can I Help My Child? Marie Collins Foundation – Sexual Abuse Online
Let's Talk About It provides advice for parents and carers to keep children safe from

online radicalisation

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

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

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

Parentzone provides help for parents and carers on how to keep their children safe 159 online

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

Support for parents/carers

National Crime Agency's CEOP Education Programme provides information for parents and carers to help protect their child from online child sexual abuse, including #AskTheAwkward, guidance on how to talk to their children about online relationships

Online safety- Remote education, virtual lessons and live streaming at Balderstone support documents.

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

Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely

London Grid for Learning guidance, including platform specific advice
National cyber security centre guidance on choosing, configuring and deploying video

conferencing
UK Safer Internet Centre guidance on safe remote learning

Guidance to support schools and colleges understand how to help keep pupils, students and staff safe whilst learning remotely can be found at Safeguarding and remote education - GOV.UK (www.gov.uk) and Providing remote education: guidance for schools - GOV.UK (www.gov.uk). The NSPCC also provide helpful advice - Undertaking remote teaching safely.

Learner Acceptable Use Agreement - Fox class and Owl class 2023-2024

Introduction

Digital technologies have become integral to the lives of us as young people, both within and outside school. These technologies are powerful tools, which open-up new opportunities for everyone. They can stimulate discussion, encourage creativity and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies. As we are moving towards becoming a 1:1 device school at Balderstone we need to ensure that we are using technologies smartly, safely and effectively.

This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

Our school mission statement is founded on the mission of '**Loving God**, **Loving Each other** and **Loving Learning**" Therefore, when I use devices, I must behave **responsibly** to help keep me and other users safe online and to look after the devices.

Love God	I will treat others as I would like to be treated online and offline, remembering that Jesus taught us to love one another as He has loved us.
Love One Another	I will remember that I need consent and agreement to use any images/information that belong to others, to show them respect, privacy and compassion.

Love Learning	I will use the technologies available in school to support my own and others' learning and not use them to distract or divert from my own or others' learning.

For my own personal safety:

- I understand that what I do online will be **supervised** and **monitored** and **reported** upon and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly
- I will only visit internet sites that adults have told me are safe to visit – using a teacher allocated search engine.
- I will keep my usernames and passwords safe and secure and not share it with anyone else (other than my parents and teacher when asked)
- I will not randomly airdrop images, documents or information to anyone else without express permission.
- I will be aware of "stranger danger" when I am online
- I will not share personal information about myself or others when online
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online. I will use the 'Home' button to close down an inappropriate screen and take the device immediately to an adult for support on reporting an issue.

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if/when I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes without permission from school.
- If you own the device and have taken it home then apps and games can be downloaded BUT not played or used within school unless directed by an adult.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do. In school, when accessing my iPad, I will only use the apps/programs that my teacher directs me to use.
- I will think about how my behaviour online/on iPad might affect other people:
- When online, I will act as I expect others to act toward me.
- I will not copy anyone else's work or files without their permission.
- I will be polite and responsible when I communicate with others and I appreciate that others may have different opinions to me.
- I will not take or share images/videos of **anyone** without their direct permission/consent.

- I will delete any unused photos/apps/files from my iPad to ensure that it can kept organised and memory space kept free for learning.

I know that there are other rules that I need to follow:

- I will only use my own personal device (iPad) in the school if I have permission.
- I will NOT use social media sites in school.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work.

I understand that I am responsible for my actions, both in and out of school:

- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules, I may be subject to disciplinary action. This could include *loss of access to the school network/internet, loss of right to use 1:1 device, suspensions, parents/carers contacted and in the event of illegal activities involvement of the police.*

Learner Acceptable Use Agreement Form

Please complete the sections below to show that you have **read, understood and agree** to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. using my school allocated/parent owned device in school
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: ..... Year group: .....

Signed: ..... Date: .....

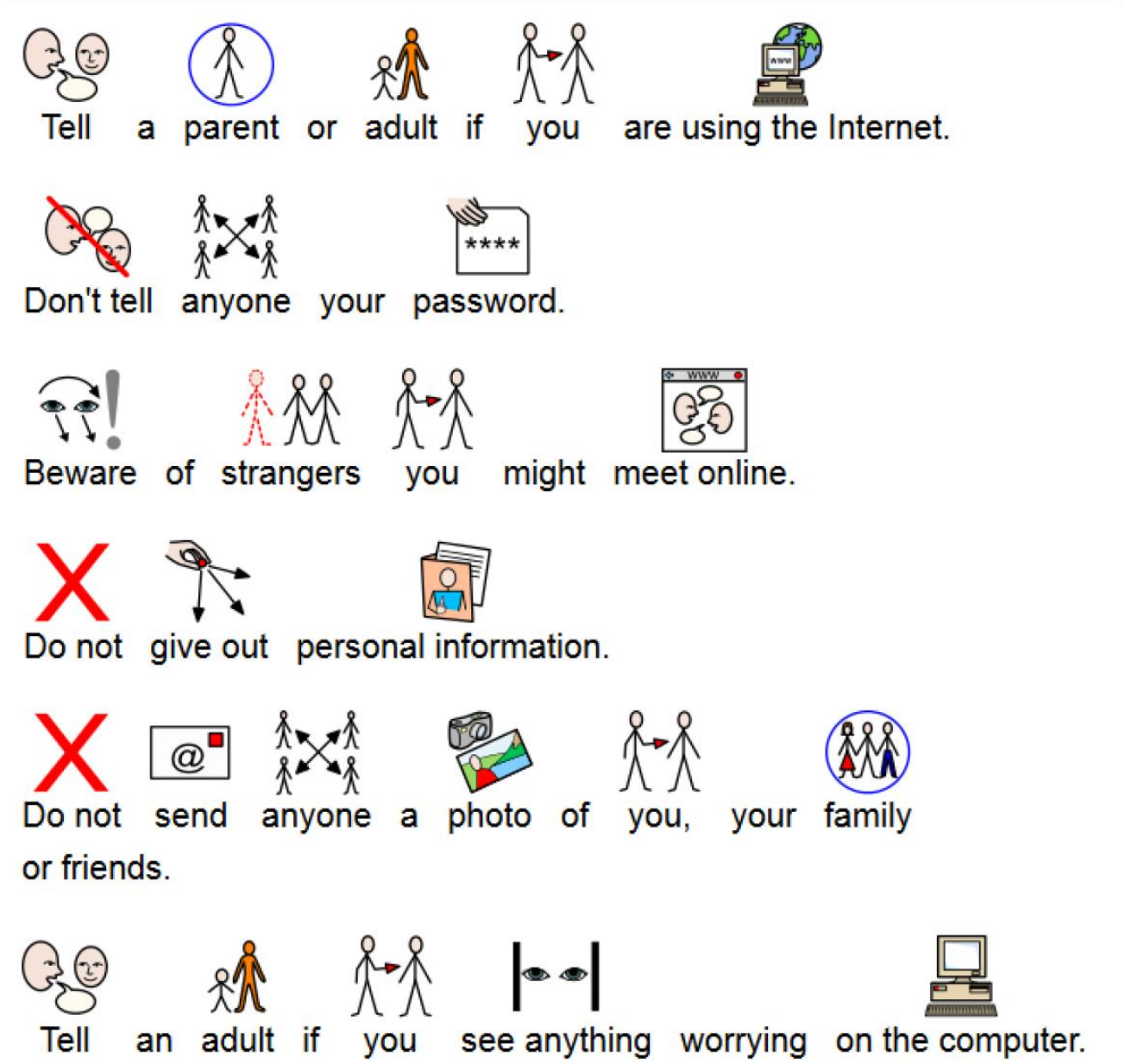
Foundation and KS1 Acceptable usage policy 2023-2024

This is how we stay safe when we use computers/iPads:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

Signed (child): .....

Signed (parent): .....



1:1 Owned iPad scheme at Balderstone St Leonard's - Introduction

Thank you so much for supporting your child's learning through the lease/purchase of an iPad for use between school/home. Balderstone is committed to innovating with educational technology to enhance teaching and learning and communication within our school community. We embrace the opportunities with which iPad technology has presented us with and permit the use of an authorised Apple iPad in a manner consistent with the established Christian mission 'Love God, Love Each Other and Love Learning' and the educational objectives of our school. We also recognise and encourage the use of the iPad for educational/leisure purposes at home.

This policy applies to all student users of Balderstone iPad hardware and software applications. It applies to all iPads used by our pupils, wherever they are physically located - within the school or used or at home. It is intended to complement Balderstone's wider safeguarding policy on E-Safety and all other relevant school policies. Due to the nature of information and communications technology, the policy will undergo periodic review and as such the school reserves the right to amend any sections or wording at any time.

The following details define the proper use of the device in school and out of school hours.

Section A – Overview of Parent Owned/leased iPad scheme

The parent/family retains ownership of all iPads, cases, accessories and apps. iPads leased by parents remain the sole property of the parent as long as all payments have been received. The School will provide all required components to ensure the iPad operates effectively in the classroom with filtered and monitored Wi-Fi access. The iPad will be connected to the school network in line with our E- Safety Policy. This means that items saved, stored or downloaded on the iPad will be hosted on the school's server.

Section B – Use of the iPad

i. Taking Care of iPads

Pupils are responsible for the general care of their iPad, case and power accessories. iPads or cases that are broken, or fail to work properly should be reported immediately. If damage occurs, the parents will be responsible for contacting the insurers to sort recompense and repair.

IPad chargers are larger than iPhone chargers and only iPad chargers should be used with the school iPads at home.

ii. General Precautions

- iPads must never be left unattended or in any unsupervised area on their own or in a school bag. Children will be given a clear place in their own trays to store their iPad during the school day.
- If left in School overnight the iPad must be left locked in the iPad trolley located in the school library (as this room is internal and double locked)
- iPads must not be put inside heavy school bags or bags with items that may damage the iPad.
- Pupils should take care of school bags with iPads in them.
- The iPad should be brought to school every day as part of regular school equipment unless directed by the class teacher to leave it at home (eg, on sports day or a trip day)

2

iii. Carrying iPads

- The school supplied protective case must be used with the iPad at all times.
- Power chargers should be left at home as the iPad should hold a charge for the duration of lessons.
- Avoid placing too much pressure or weight on the iPad screen with workbooks or folders especially if stored in full or heavy school bags.
- Please be cautious is carrying water bottles in school bags to ensure no damage to the iPad as a result of a spill/leak.
- Pupils will NOT be allowed uncapped water bottles on the class tables when the iPads are in use.

- iPads are intended for use at school each day. Pupils are responsible for bringing their iPad, **fully charged** or with charge over 80%, to school each day.
- Spare iPads will not be available to pupils who forget to bring their iPad to school or who fail to charge their iPad.
- At all times, the class teachers' decision is final regarding use, or non-use of iPads, collectively or individually.
- Sound must be muted at all times unless permission is obtained from the teacher for instructional purposes.
- Only apps provided by School in the Self Service app and school profiles may be placed on the iPad. School profiles are applied by the mobile device management system (currently with MCC digital services)

v. Using iPad at school (Photographs/Images, video and audio)

- Photographs may only be taken on the iPad when authorised by a member of staff in relation to school work. The iPad cameras are not to be used at any other time to save space and misuse of the iPad.
- Photographs/Images stored on the iPad will be in accordance with this and the School's Acceptable Use of the Internet Policy. The School reserves the right to randomly check any iPad for unsuitable content/unauthorised photos without consent.

- No images, audio or video recordings taken with a school iPad may be uploaded from any device to social networking sites by pupils or parents.
- Recording of Balderstone staff or other pupils is prohibited unless specifically permitted by the class teacher and/or the member of staff to be photographed, audio or video recorded.

vi. Charging the iPad Battery

- iPads must be brought to school each day in a fully charged condition. Pupils need to charge their iPads each evening. It may take up to 3 hours to fully charge the iPad.
- Only authorised Apple chargers must be used to ensure that no device damage occurs.
- iPads can be turned off or put into airplane mode when they are not required to save battery power.

vii. Accounts, Passwords and AppleID's

- iPads work with a School Managed AppleID, specific to its allocated user. These Apple ID's are managed by the school.
- All account details should be kept secure by the owner. Pupils are prohibited from sharing this password with anyone else except their parents or as requested by teaching/support staff.
- Pupils may not attempt to access other student or staff accounts or iPads at any time or Airdrop messages or files without permission.

viii. Home Use

- Pupils are allowed to use their iPads outside of school with Parent/Guardian consent. The iPad can connect to other wireless networks to assist them with home learning.
- The most effective filtering and safety provision for safe iPad use is parental supervision. School would advocate use of the iPad in a social space in the home, where adults are easily accessible and can monitor the child's usage of the iPad and visited websites.
- Search histories are NOT to be deleted from iPads at any time.
- **It is the responsibility of the Parent/Guardian to monitor and oversee iPad use outside of school i.e. within the home setting.**
- It is advised that digital devices such as school iPads be charged overnight away from bedrooms to avoid children accessing them unsupervised.
- Parents are advised to check, update and install their own filtering system on their home broadband provider to ensure that appropriate filters are in place at home to keep your child safe.
- Parents are advised to use and set up the Jamf parent app to manage and restrict device use at home.

x. Software and Apps

- The school's mobile device management system audits the iPads daily gathering data on installed apps, web clips, profiles that are on the iPads.

- Periodic checks will be made to ensure the iPads are being kept up to date and are in a useable state.

xi. Software Updates

- The operating system will show that updates are available from time to time with a red dot on the Settings icon. Pupils are expected to allow iOS updates a few days after they become available and should update at home when the iPad is charging OR in school during the day.
- Upgrade versions of apps are available from time to time. Pupils will be expected to allow these updates when they are available.
- If there is a difficulty with update to iOS or apps make sure there is enough free space on the device to all them to install. Apps can be removed and added again via Self Service. Documents, videos and photos can be uploaded to cloud storage and then removed from the device.

xii. Procedure for reloading software

- If technical difficulties occur or illegal apps or networking profiles (e.g. non School approved) are discovered, the iPad will be reset. The school does not accept responsibility for the loss of any software or documents deleted due to a re-format and re-image.
- Resetting iPads is a last resort measure carried out only if necessary when other solutions fail.

xiii. Inspection

- Pupils may be selected at random to provide their iPad for inspection to ensure they comply with the E-Safety Policy and the Acceptable Use of the Internet Policy.

Section C - Acceptable Use Section

In addition to the School's Policy on the Acceptable Use of the Internet, the E-Safety Policy, the School permits use of an Apple iPad in a manner that supports the School's aims and objectives and is in line with all School policies.

This policy is provided to make all users aware of their responsibilities associated with efficient, ethical, and lawful use of technology resources. If a person violates any of the user terms and conditions named in this policy, privileges may be terminated, access to the School's network may be denied, and the appropriate disciplinary action shall be applied in line with the school's policies on the Acceptable Use of the Internet and the Positive Behavioural Policy.

i. Parent / Guardian Responsibilities

Parents are expected to talk to their children about the values and standards that they should follow on the use of the Internet and online services just as they do on the use of all media information sources such as television, books, movies, radio, telephones, advertisements etc.

Parents and pupils should familiarise themselves with the details in section B in case of accidents, theft or misuse.

(ii) Student responsibilities:

Use an iPad in a responsible and ethical manner;

Obey general School rules concerning behaviour and communication that apply to all digital devices and their use;

Use all digital school resources in an appropriate manner
Turn off and secure their iPad after they are finished working to protect their work and information;
Report any app or system containing inappropriate content or questionable material;
Report any page containing inappropriate or abusive language or if the subject matter is questionable;

iv. Prohibited Activities

In addition to the guidance outlined in the School's wider policy on Acceptable Use of the Internet pupils are not permitted to:

v.

- Use or take another student's iPad;
- Use a staff member's iPad without consent
- Use other's usernames or passwords;
- Trespass in other's accounts including email, folders or files;
- Take any photographs, video or audio recordings other than those directed by a member of
- staff Upload any photo, audio or video content taken to any social networking sites.
- Use the school's Apple TVs without a staff members consent or when unsupervised
- Stream video or audio i.e. live radio when not part of a taught lesson
- Airdropping to others without prior consent
- Download illegal content or material which is inappropriate;
- Attempt to 'Jailbreak' their iPad;
- Send or display offensive messages or material;
- Install or transmit copyrighted materials;

- Use abusive/inapropriate language or content;
- Damage devices, computer systems or computer networks;
- Change iPad settings (exceptions include personal settings such as font size, brightness, etc)

Legal Propriety

Pupils should comply with trademark and copyright laws and all license agreements. Ignorance of the law is not immunity. If a parent/pupil is unsure, they should ask a teacher or parent.

Use or possession of hacking software is strictly prohibited and violators will be subject to sanctions. Violation of the law may result in criminal prosecution or disciplinary measures.

iPad Identification

Student iPads will be labelled in the manner specified by the School. iPads can be identified in the following ways:

- The device name in Settings -> General -> About should match the student's username
- The device Serial Number

vii. Disciplinary measures

Any student who persistently refuses to co-operate or violates any aspect of the provisions of this policy or the Acceptable Use of the Internet Policy may face disciplinary action deemed appropriate in keeping with the school's Positive Behavioural Policy.

viii. Staff Action

A student will be required to hand over their iPad to a member of staff if:

- the iPad is not being taken care of appropriately.
- there is a suspicion that the iPad has unsuitable material stored on it;
- a student has disrupted learning through improper use of an iPad;
- a student has misused their iPad to take photographs, video or audio recording on the school premises for which they have not received permission.
- the iPad or any of its features has been used for any form of bullying;
- games are being played on the iPad during class time without permission;
- the iPad is being used to stream video or audio outside of a class lesson at teacher direction;
- the iPad has been used to breach any school rule or goes against the school's Christian mission

Student and Parent/Guardian Agreement Form

Please complete the form on page 8 and return it to the class teacher. By signing, the Student and Parental/Guardian Consent Form you are agreeing to abide by the School Owned iPad Pupil Acceptable Use Policy and Procedures, the E-Safety Policy and the Acceptable Use of the Internet Policy. This agreement lasts for the entire enrolment at Balderstone in KS2.

This policy may be updated/amended. New versions of this policy may be found on the School website or a hard copy will be available through the school office.

Outside of the scheduled review of this policy, parents will be informed of changes via Parent mail.

iPad Agreement Form

Please complete the sections on this page and return to Mrs Riddell or Mrs Turner.

Student Section:

I accept and will adhere to the guidelines and conditions outlined in the School Owned iPad Pupil Acceptable Use Policy (AUP) and Procedures

Student name: (please print clearly)

Student Signature: _____

Date: _____

Parent/Guardian Section:

I have read and agree to the conditions outlined in the School Owned iPad Pupil Acceptable Use Policy (AUP) and Procedures

Parent / Guardian name: (please print clearly)

_____

Date: _____