BRETHERTON ENDOWED CE PRIMARY SCHOOL
Online Safety Policy

Walking in the footsteps of Jesus with our Christian family, we learn, grow, achieve and flourish together in God's love.

This policy is for Bretherton Endowed CE Primary School and The Hub, Bretherton Endowed Out of School Provision.

We recognise that:

- the online world provides everyone with many opportunities and is both an integral and valuable part of life today; however it can also present risks and challenges
- we have a duty to ensure that all children and adults involved in our school are protected from potential harm online
- we have a responsibility to help keep children and safe online, whether or not they are using our school's network and devices
- working in partnership with children, their parents, and other agencies is essential in promoting young people's welfare and in helping them to be responsible in their approach to online safety
- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

Aims

Our school aims to:

- Have a whole school approach to online safety that includes all staff, parents, pupils and governors.
- Equipping school staff, parents and children with the most up to date knowledge they need to understand online dangers and how best to react should an incident arise.
- Educates and empowers children to enjoy the internet but also understand the dangers and risks.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them

for sexual, criminal, financial or other purposes

- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and **online bullying**
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

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

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

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

Roles and responsibilities

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports.

Online safety governor : Laurence Glew

The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Lead
- supporting the full governing body in making strategic and informed decisions regarding schools filtering and monitoring systems through their understanding and online safety governor report
- complete with the computing lead / Head the online safeguarding audit annually
- review reports from the Online Safety Lead and monitor progress of online action plans
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to full Governors

Headteacher

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.

The Headteacher is responsible for ensuring that the Online Safety 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. In addition, the Headteacher will ensure that staff are trained and aware of their responsibilities in relation to their professional conduct including professional online practice.

The Headteacher 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 Headteacher and Online Safety Lead will liaise regularly for collating and monitoring reports. In this, they will monitor the effectiveness of this policy and make updates in accordance with national or local changes or needs. These changes will be communicated to staff through the start of staff meetings

The Headteacher with expertise from IT support company (Currently Virtue Technologies) is responsible for:

- ensuring the school's technical infrastructure is secure and is not open to misuse or malicious attack- Netsweeper
- that the school meets required online safety technical requirements and follows Lancashire guidance
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (**see Appendix 1**)
- that monitoring software/systems are implemented and updated

The headteacher in conjunction with SLT and governors is also responsible for writing and ensuring that all staff and volunteers read and understand the:

- Staff professional ict responsibility policy
- Mobile phone policy for staff and visitors
- Remote learning policy
- Twitter policy
- Managing the media policy
- ICT safe user policy- visitors and volunteers
- Personal data handling policy
- Child Protection Policy

Online Safety Lead

The Online Safety lead will take a day to day responsibility for online safety.

They will:

- Take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents.
- Keep their own subject knowledge and skills upto date ensuring a high level of competence
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place. **Appendix 2**
- Provide in house training and advice for staff where needed.
- Receive reports of online safety incidents and create a log of incidents to inform future online safety developments and needs using Google Forms. **Appendix 3**
  Write a termly report for the online safety governor and meet regularly with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs.
- Attend relevant meetings of Governors and ensure governors are fully up to date with current online safety procedures in place.
- Report to and liaise regularly with the Headteacher

Designated Safeguarding Leads- Head and Deputy head.

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
- inappropriate on-line contact with adults/strangers

- potential or actual incidents of grooming
- online-bullying

Our DSL : Alison Moxham (Head) Deputy DSL: Jayne Clarke

Currently this training will form part of our annual safeguarding training, updates from national online advice, National Online Safety Platform, Local Authority updates. Training will be updated in our school CPD document and / or DSL meeting minutes.

All staff

All staff are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms of the staff professional ICT responsibilities policy **(Appendix 8),** mobile phone policy for staff and visitors, remote learning policy, personal data handling policy
- Ensuring that pupils follow the school's terms on acceptable use/ 1-1 device agreement and the golden rules for computing
- Challenging any inappropriate behaviour online (radicalisation, cyber crime, cyberbullying, peer on peer, upskirting, sending nude, semi nude photographs, inappropriate content)
- Working with the DSL and Online Safety lead to ensure that any online safety incidents are logged via Cpoms and our online safety reporting form and dealt with appropriately in line with this policy **(Appendix 2 and 3)**
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

Students/Pupils:

- Are responsible for using digital technology systems in accordance with the pupil acceptable use agreement
- Realise that the school's online safety policy covers their actions in and out of school
- Must follow and adhere to our 'golden rules' **Appendix 4**
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so by following our golden rules and using the online reporting button **Appendix 5**
- Sign and adhere to the Home- School Agreement for devices acquired through the school **Appendix 6** and the 1-1 device agreement. **Appendix 7**

Parents/carers

Parents/carers play a crucial role in 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 workshops, newsletters, letters, website, social media and information about national/local online safety campaigns/literature.

Parents and carers will sign and support their children in adhering to the Home-school agreement **(Appendix 6)** and the 1-1 device agreement **(Appendix 7)**

If their child/ children needs to work from home due to isolation, they will follow and support them in adhering to the Remote Learning Policy.

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
- access to parents' sections of the website and online learning
- their children's personal devices in the school and at home

Volunteers, visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of the ICT safer user policy for visitors and volunteers and the mobile phone policy. They will be expected to read and follow them.

Education & Training

Educating Staff

It is essential that all 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 Online Safety Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations. This will include self -initiated learning opportunities through forums and national initiatives

This online safety policy and its updates will be presented to and discussed by staff in staff meetings. All adults in school following this policy will collaborate in it.

The Online Safety Lead or Headteacher will provide advice/guidance/training to individuals as required.

Educating pupils

At Bretherton, we believe Online safety is vital and staff should reinforce online safety messages **across** the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

Pupils will be taught explicit lessons about online safety as part of both our computing and PSHE and RSE curriculum:

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

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

All schools have to teach:

- Relationships education and health education in primary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

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

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance

of respect for others online including when we are anonymous

- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

- In addition to teaching online safety through our curriculum, key online safety messages will be reinforced as part of a planned programme of assemblies and initiatives such as Internet safety day
- Pupils will be 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 will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils will be 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 decision-making.
- Staff will act as good role models in their use of digital technologies, the internet and mobile devices.

Where necessary, teaching about safeguarding, including online safety, may be adapted for vulnerable children, victims of abuse and some pupils with SEND. Teaching may be adapted for individuals who may be deemed at additional risk eg vulnerable children

Educating parents

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. Parents will have access to the National Online Safety Platform and be directed to relevant material there. Online safety will be highlighted through parents workshops.

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

Concerns or queries about this policy can be raised with the DSL or the Computing subject leader.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy and anti- bullying policy)

Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes.

Teaching staff know where to find opportunities to use aspects of the curriculum to cover cyber-bullying in both our Computing and PSHE curriculum. Staff will be directed to the NOS platform for up to date and relevant information or changes.

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

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

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

All cyber bullying incidents will be reported to DSL through CPOMS and / or online safety reporting form

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Peer on Peer Abuse

All children are capable of abusing their peers. This can manifest itself as:

- bullying including online bullying
- sexting, sexual harassment online- inc sharing nude/ semi-nude pictures
- inappropriate relationships on social media
- initiation/hazing type violence and rituals
- County lines - a network between an urban centre and county location where drugs are sold often over a mobile phone. Children and vulnerable people are used to transport drugs, cash or even weapons. It can involve intimidation, blackmail and serious violence.

Staff are up to date on safeguarding training and are fully aware of all forms of peer on peer abuse. This is clearly outlined in our child protection and safeguarding policy.Staff are clear to report any issues involving peer on peer abuse using Cpoms and to the DSL. The headteacher and online safety leads receive weekly filter prevent reports which immediately inform us of any suspicious search behaviour. Children can report concerns through our pupil online safety button or approach any member of staff where they know they will be listened to and treated seriously and acted on accordingly.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (**See appendix**). Visitors will be expected to read and agree to the ICT Safer Use Policy for visitors and volunteers. Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

Netsweeper (as part of BTLS Lancashire broadband offer) monitors the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Pupils using mobile devices in school

Pupils are not permitted to bring mobile devices into school unless a prior agreement has taken place between parents and school, often surrounding the child's safety when travelling to and from school. Any mobile phones brought in must be kept in the school office during school hours. At no time is a pupil permitted to use their mobile device on school premises.

Staff using work devices outside school

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of

upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)

- Making sure the device locks if left inactive for a period of time
- Ensuring personal data is not available to unauthorised sources under GDPR regulations
- Not sharing the device among family or friends
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the Staff's Professional ICT Responsibilities Policy, as set out in **(Appendix 8).**

Data protection/ GDPR- Linked to Personal Data Handling Policy.

When personal data is stored on any mobile device we will ensure that:

• the device is to be password protected. (be sure to select devices that can be protected in this way)

• device must be protected by up to date virus and malware checking software

Staff will ensure that they:

• at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse

• can recognise a possible breach, understand the need for urgency and know who to report it to within the school

• where personal data is stored or transferred on mobile devices these must be password protected.

• will not transfer any school personal data to personal devices

• access personal data sources and records only on secure password protected computers and other devices

Reporting internet misuse or online safety breeches

At Bretherton, we have robust procedures in place to ensure a safe and secure approach to the management of incidents. All staff to be aware of these and use a professional approach at all times. However, incidents that might involve illegal or safeguarding issues should be reported to DSL immediately and will be followed using the right hand side of the flow chart. In reality at Bretherton Endowed, the DSL will have all online safety breaches reported to them through CPOMS, online safety report form and /or verbally.

See appendix- flow chart. **Appendix 2**

How the school will respond to issues of misuse.

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

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

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

Training

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

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

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

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

online abuse

• Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

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

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

Volunteers will receive appropriate training and updates, if applicable.

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

Monitoring arrangements

The DSL reviews and logs behaviour and safeguarding issues related to online safety that has been reported through Cpoms from the online safety reporting forms.

Pupil's understanding and application of our online safety policy will be reviewed through pupil questionnaires and low stakes quizzes in computing and PHSE/RSE lessons

Parents understanding will be reviewed regularly through parent forums and parental workshops and questionnaires

Updates and Bretherton Endowed Primary School adoption of updates will be discussed, shared with staff through staff meetings and minuted in DSL termly meeting and / or online safety governor reports.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Anti-bullying policy
- Staff disciplinary procedures
- Complaints procedure
- Staff professional ict responsibility policy
- Mobile phone policy for staff and visitors
- Remote learning policy
- Twitter policy
- Managing the media policy
- ICT safe user policy- visitors and volunteers
- Personal data handling policy
- Protecting your data policy (GDPR)
- Computing subject policy
- PHSE and RSE subject policy

Written by- S. Allchurch- Online Safety Lead

Adopted by the governing Body : May 2022 To be reviewed :Annually

Headteacher : Mrs Alison Moxham Chair of Governors : Mr T. G. Wilson www.brethertonschool.org.uk

Appendix 1- Filtering Policy

Bretherton Endowed CE Primary School Filtering Policy

"Walking in the footsteps of Jesus with our Christian family, we learn, grow, achieve and flourish together in God's love."

This policy is for Bretherton Endowed CE Primary School and The Hub, Bretherton Endowed Out of School Provision.

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of the Head teacher with the support of Virtue Technology.

Technical Security

Policy statements

The school will be responsible for ensuring that the school infrastructure 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 receive guidance and training and will be effective in carrying out their responsibilities.

- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **Appropriate security measures are in place (See Appendix 1) to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.**
- **Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff (See Appendix 2)**

- **All users will have clearly defined access rights to school technical systems.(See Appendix 3)**
- Users will be made responsible for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. (see password section below)
- The school bursar is 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
- Mobile device security and management procedures are in place (See Online safety policy)
- 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. (See Appendix 4)
- Remote management tools are used by senior staff to control workstations and view users activity
- An appropriate system is in place for users to report any actual / potential technical incident to the Online Safety Coordinator / Network (See Appendix 5 5:1)
- An agreed policy is in place (See Appendix 6 6:1) for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system.
- An agreed policy is in place (6:2) regarding the downloading of executable files and the installation of programmes on school devices by users
- An agreed policy is in place (6:3) 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.
- An agreed policy is in place (See Appendix 7) regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices.
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

- Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Online Safety Group (or other group).
- **All school / academy networks and systems will be protected by secure passwords that are regularly changed**
- **The "master / administrator" passwords for the school systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place eg school safe.**
- All users (adults and young people) will have responsibility for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords for new users, and replacement passwords for existing users will be allocated by request to Virtue Technology. This will be recorded in the 'events log' in Appendix 8.
- Users will change their passwords at regular intervals

Staff Passwords

- **All staff users will be provided with a username and password** by Virtue Technology technician who will keep the up to date record of users and their usernames updated in school office.
- the password should be a minimum of 8 characters long and must include – uppercase character, lowercase character, number and/or special characters
- passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
- should be changed at least every 60 to 90 days and should not re-used for 6 months and be significantly different from previous passwords created by the same user.

- Student / Pupil Passwords
- Previously children were allocated a username and password allocated by Virtue for access to a windows device. Bretherton Endowed in conjunction with parents have rolled out a chromebook 1 to 1 device scheme. This means that children no longer require a windows network login. **(See Google admin section below)**
- Children will continue to be taught the importance of password security

Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users.

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's online safety policy and password security policy
- staff meetings and regular updates
- through the Acceptable Use Agreement

Children will be made aware of the school's password policy:

- in computing lessons
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The responsible person (Head Teacher) will ensure that full records (manual or automated) are kept of:

- User Ids and requests for password changes
- User log-ins
- Security incidents related to this policy

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

We will:

- use the provided filtering service without change or but allow flexibility for sites to be added or removed from the filtering list for their organisation
- No differentiated filtering for different ages of users will be provided

Responsibilities

The responsibility for the management of the school's filtering policy will be held by Head teacher along with the Online Safety Governor. They will manage the school filtering, in line with this policy and will keep records of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must :

- **be logged in change control logs**
- **be reported to a second responsible person (** Online Safety Governor via termly report)

All users have a responsibility to report immediately to The Head teacher any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering systems in place to prevent access to such materials. Such reference is made to the Mobile phone policy.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists . Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The school maintains and supports the managed filtering service provided by the Internet Service Provider - NetSweeper
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the Head teacher and the details will be documented for the online safety governor termly report.

Education / Training / Awareness

Children will be made aware of the importance of filtering systems through the online safety education programme included in our computing curriculum.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions / website links, newsletter etc.

Changes to the Filtering System
In this section the school should provide a detailed explanation of:

- how, and to whom, users may request changes to the filtering the grounds on which they may be allowed or denied
- the use of the Governotr termly report as a log of changes
- any audit / reporting system

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Headteacher who will decide whether to make school level changes. The Headteacher, Deputy Head Teacher and Computing lead are staff in school with access to the Admin area of Netsweeper.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement. *Monitoring will take place as follows:*

- *Termly reports to governors from Netsweeper filtering service listing breaches and recording key areas of concern.*
- *Weekly reports sent from Netsweeper identifying IP address and content filtered or declined.*
- *Observational supervision of children during in class activities.*
- *Routine (at least half termly) class teacher checks on history and recent searches.*
- *One off searches of history if alert to concerns.*

Audit / Reporting
Logs of filtering change controls and of filtering incidents will be made available to:

- the second responsible person (Onliine Safety Governor via termly reports) which will feed into curriculum and standards committee
- External Filtering provider / Local Authority / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

Further Guidance
We have sought guidance: *"to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"* (Revised Prevent Duty Guidance: for England and Wales, 2015).

KCSE *"ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges 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."

In response UKSIC produced guidance on – information on "Appropriate Filtering"

NEN Technical guidance: http://www.nen.gov.uk/e-security-managing-and-maintaining-e-securitycyber-security-in-schools/

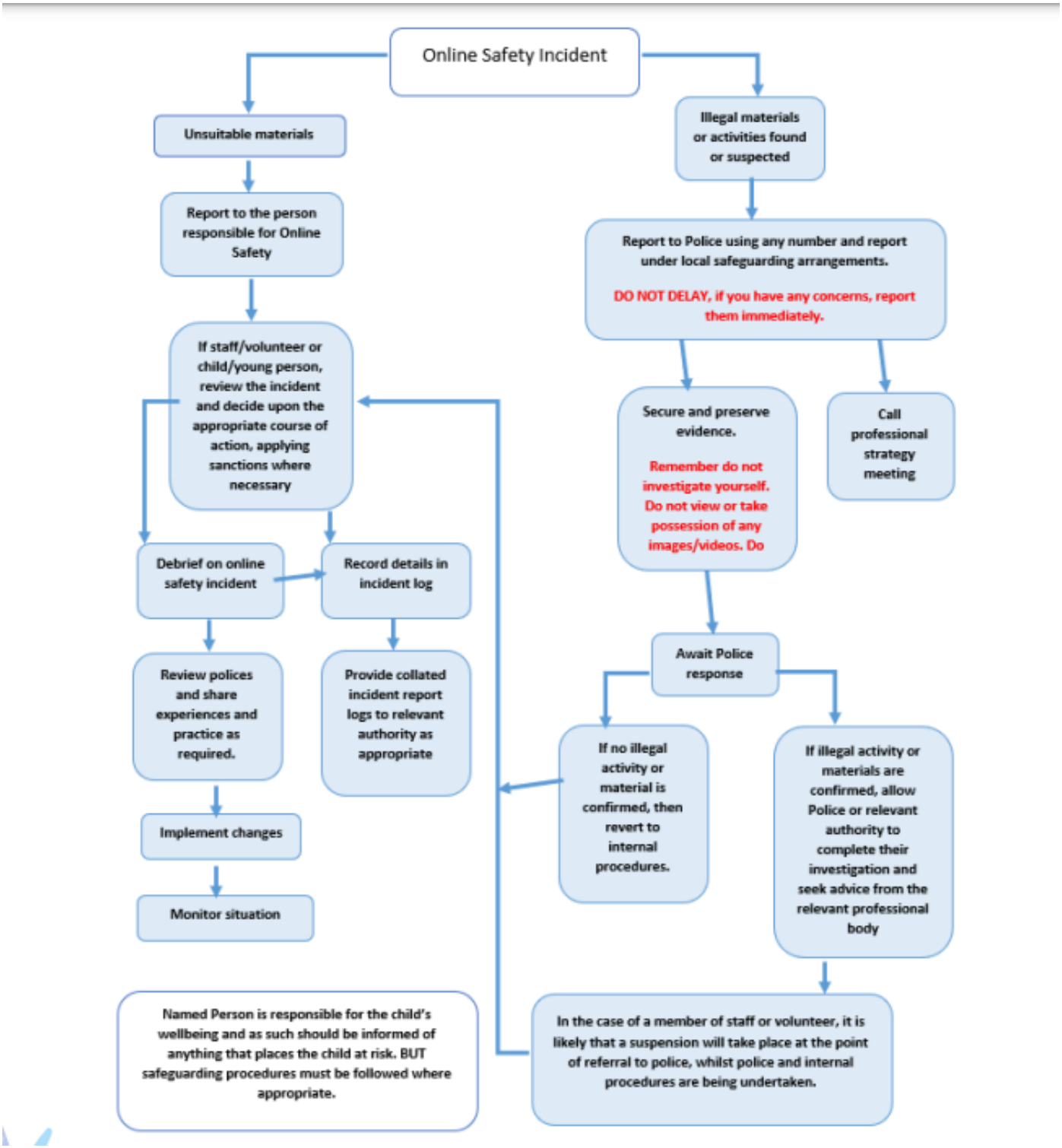
Somerset Guidance for schools – this checklist is particularly useful where a school / academy uses external providers for its technical support / security: https://360safe.org.uk/Files/Documents/Somerset-Questions-for-Technical-Support-v4.aspx

Adopted : November 2021

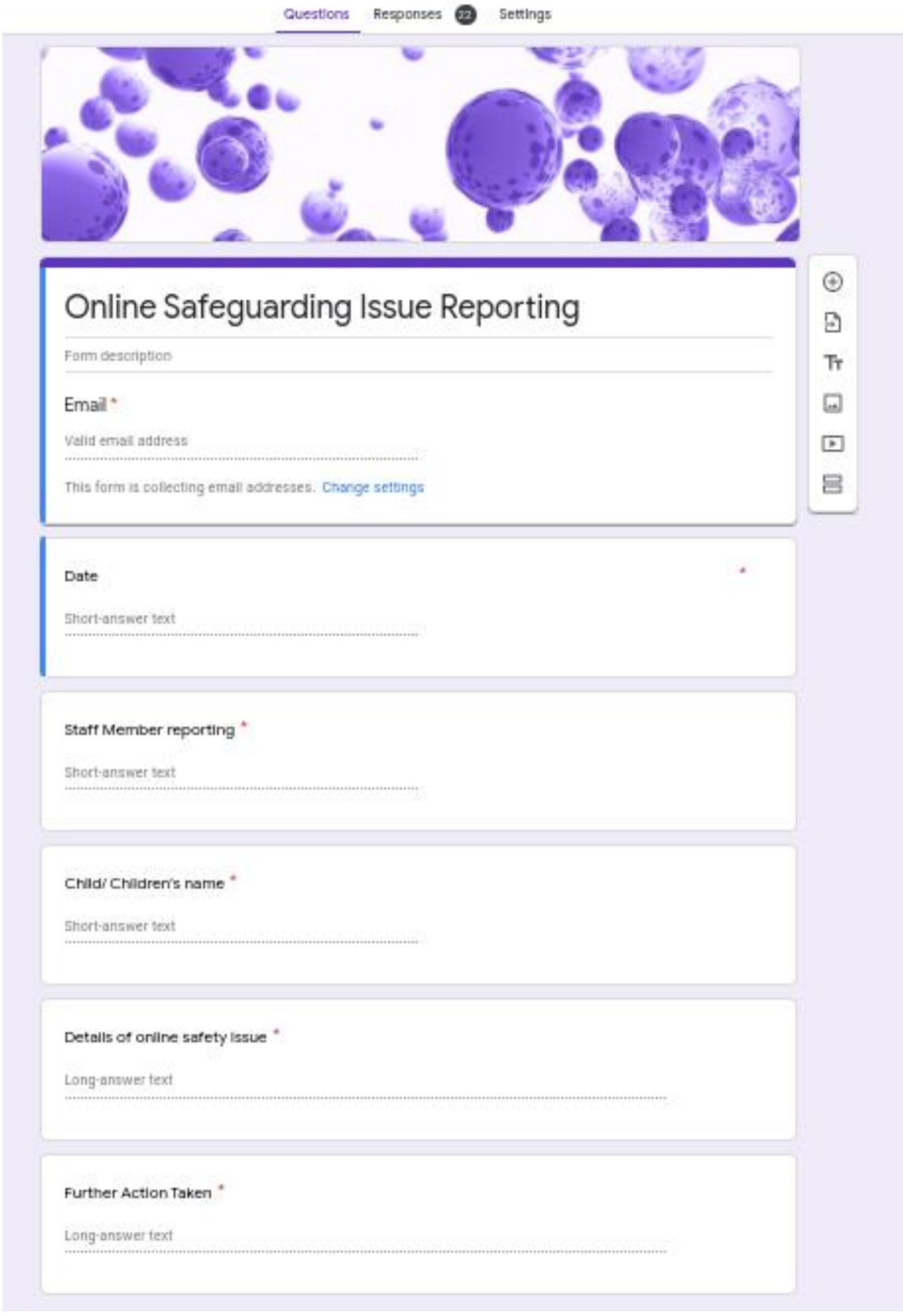
To be reviewed :No later than the end of 2023

All aspects of our policy intends to comply within the Data Protection (GDPR) legislation.

Appendix 2 Reporting internet misuse or online safety breeches

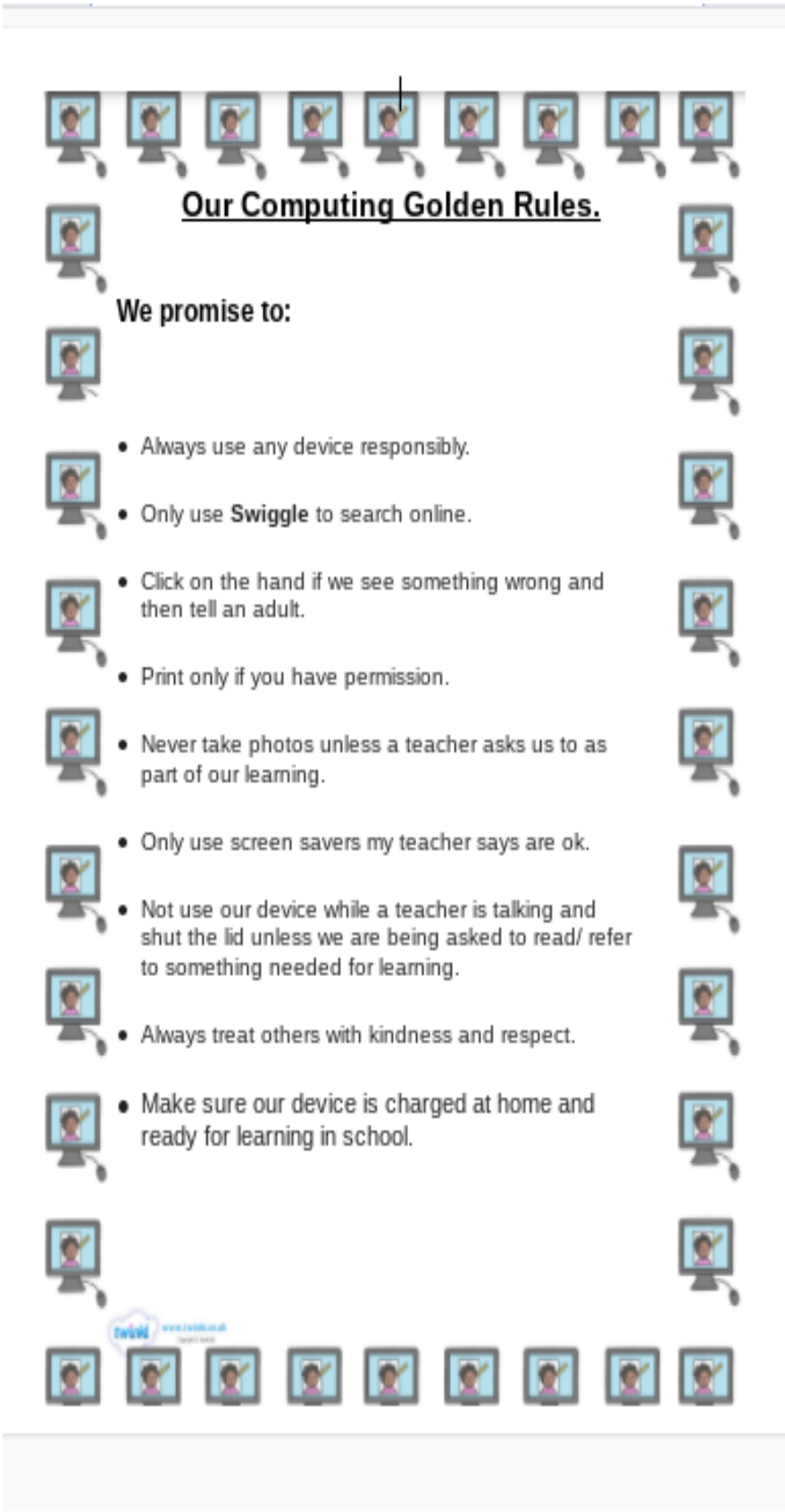


Appendix 3

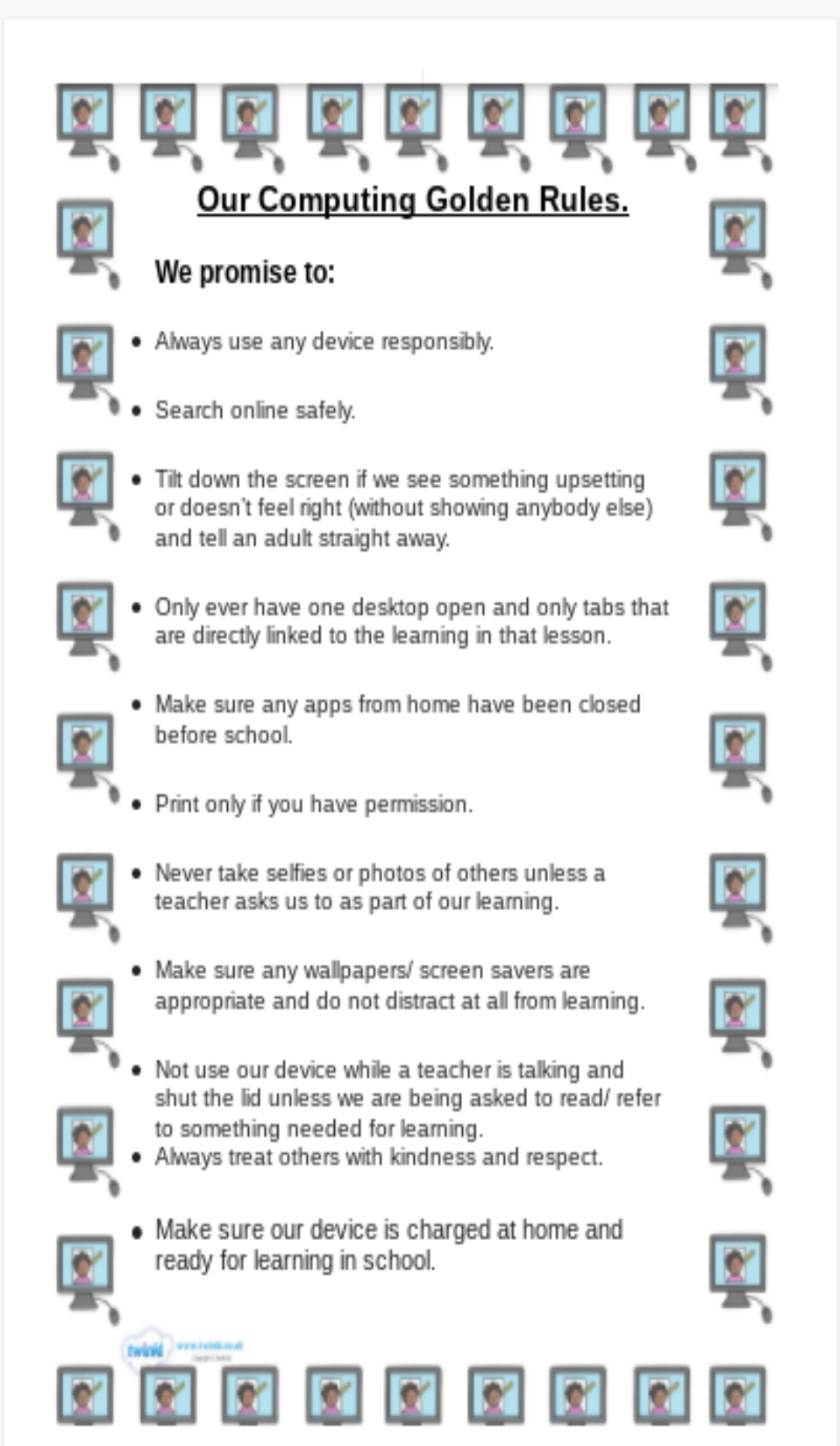


Appendix 4

Class 1 and 2 Golden Rules.

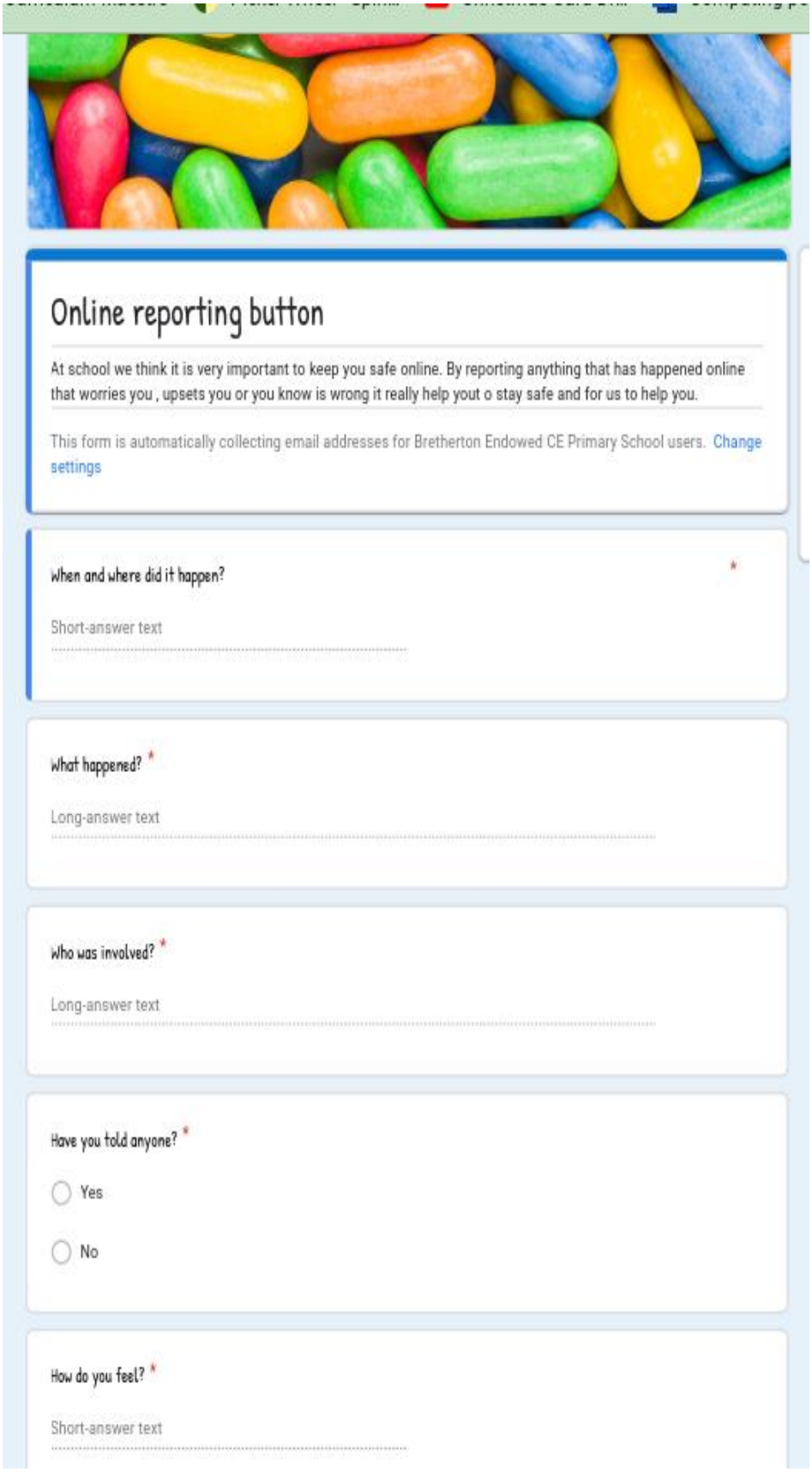


Class 3 and 4 Golden Rules.


Our Computing Golden Rules.
We promise to:
Always use any device responsibly.
Search online safely.
Tilt down the screen if we see something upsetting or doesn't feel right (without showing anybody else) and tell an adult straight away.
Only ever have one desktop open and only tabs that are directly linked to the learning in that lesson.
Make sure any apps from home have been closed before school.
Print only if you have permission.
Never take selfies or photos of others unless a teacher asks us to as part of our learning.
Make sure any wallpapers/ screen savers are appropriate and do not distract at all from learning.
Not use our device while a teacher is talking and shut the lid unless we are being asked to read/ refer to something needed for learning.
Always treat others with kindness and respect.
Make sure our device is charged at home and ready for learning in school.

Appendix 5

Children's online reporting button.



Appendix 6

HOME SCHOOL AGREEMENT

Bretherton Endowed CE Primary School

Home School Agreement for e-learning Programme

Using technology in school and at home brings learning right into the 21st century. It gives learners the opportunity to learn at their own pace, and for learning at home to be more structured and effective.

We believe that this technology will give every learner the opportunity to progress faster and achieve more. We also believe that it will help to strengthen relationships between home and school.

HOME SCHOOL AGREEMENT

To help ensure that e-learning is a big success at Bretherton Endowed CE Primary School and that we get maximum value from our *joint* investment in your children, we invite you to commit to the principles outlined in this agreement. As a school we are prepared to provide all of the back-up and resources needed to make this work, but we also need the commitment of parents and students.

As you read through this leaflet you will see a summary of the e-learning commitment that the school is making to the students and to you as parents. It also outlines the commitment that will be needed from the home, and from the children themselves, to make this work.

When you have read these sections we invite you and your child to sign the agreement and return it to school. This will help to ensure that we are all working together to achieve success.

Remember that using a chromebook (referred to as the 'device' in this leaflet)carries with it a level of responsibility to work in an ethical manner at all times.

TERMS & CONDITIONS

- Failure to take reasonable care or to abide by the other conditions in this document may result in the device being reclaimed. The school reserves the right to claim financial recompense in such cases
- The device should be charged at home overnight, and parents take responsibility for any associated electricity costs.
- The device and its software will remain the property of the school until the end of the loan period
- Ensure that the device is returned either at the end of the programme or if the student leaves the school if an agreement to complete the donations cannot be found.

THEFT:

A stolen device must be reported to the school as soon as possible when you will be required to fill in a Theft form. From there the police will be notified within 48 hours of notification of theft and a crime number assigned. We will not cover the cost of replacing the device under the following circumstances:

- The device was left in plain view in an open bag or unlocked locker, car or house
- The device was stolen due to negligence, careless behaviour or unwise use in or out of school

---

SOFTWARE:

School will promote educational apps and software and provide for them within school. These may be accessed at home. Parents are able to upload software onto the devices but not through the school google account and MUST be appropriate to the age of the child.
Children will be reminded that they can only access school accounts in school.

THE SCHOOL WILL*:

- Provide a device for your child's use, for the length of the programme
- Provide a case to protect the device
- Provide the Apps and Resources required for educational purposes

- Make sure that the device is covered by insurance for use in and out of school for study purposes, providing reasonable care is taken to prevent loss (through theft) or damage
- Provide secure storage for the device when it is not needed for any particular lesson
- Provide on-going support for the device
- Give parents and learners a proper introduction to using and caring for the device & software
- Teach students to use the device safely
- Monitor the use of the device directly in and around school

*through facilitating the donations from parents.

AT HOME WE WILL:

- Ensure that our child understands how to care for and protect their device
- Report any loss or damage (including accidental loss or damage) within one week
- Report any faults in hardware or software promptly
- Ensure that your child understands that the device is primarily for educational purposes and that it is always in a state to work with
- Ensure your WiFi at home has adequate filters to safeguard your child's access to apps and the internet.
- Promote online safety and promote responsible use in interactions and general use

---

AS A STUDENT I WILL:

- Look after my device very carefully all of the time. It will be kept in its case and stored securely when not in my possession
- Take responsibility for setting up a secure password through @bretherton.lancs.sch.uk account and not sharing it with other students
- Bring it to school every day fully charged, unless I have been told not to
- Take care when the device is transported so that it is as secure as possible (e.g. not visible in a vehicle / not left in school backpacks out of view)
- Not carry water bottles in the same bag as the device unless the bag has an integrated but separate (waterproof) compartment specifically for transporting bottles.
- Keep in its case when not being used and this is kept in good repair.
- Make sure the device is not subject to careless or malicious damage (e.g. as a result of silliness)
- Ensure my device is only used for educational purposes whilst in school
- Regularly update my device as instructed by the school
- Allow staff to access the device to check for inappropriate materials. I understand that staff will be allowed to remove inappropriate resources
- I will always act on the advice of the school in the safe use of this device

---

AS A STUDENT I WILL NOT:

- Use my device for any form of cyber bullying or for sending, accessing, uploading or distributing any insulting, threatening, inappropriate, violent material
- Use my device for sending mass emails (spamming)
- Use my school email account for any form of commercial or financial gain
- Create a separate profile and use this within school
- Take photographs or videos without the permission of the subject. I will not upload or share these images with anyone without the permission of the subject
- Install age-inappropriate games and content
- Physically decorate, customise or use graffiti on the device or it's case
- Delete any software I have been asked to install
- Use my device for any illegal and/or anti-social purpose, including access to inappropriate websites

---

BROKEN DEVICE:
Unfortunately, devices on occasion do get broken and this is the procedure should the need arise.

A broken device must be reported straight away as we only have a week's window to claim on the insurance, even if it is during the holidays. All breakages must be reported even if it is a tiny crack in the screen and a form must be completed. If an item is still within the 3 year warranty period, you should follow the warranty returns process.
The insurance only permits a maximum of two claims without excess every policy year.

We will not support the following breakages and therefore you will be required to pay for them:

- Deliberate and wilful damage to the device
- Any problems resulting from devices that have been 'Jailbroken'

During the time it takes to repair the device we have a limited stock of loan devices for use during the school day which must be returned after the last lesson
Please ensure that you have received the Compucover summary of insurance document attached to this agreement.

Please sign this tear off slip and return it to the school at the same time as you collect your device. :-

STUDENT'S AGREEMENT
I agree to abide by these terms in my use of the Chromebook

Name: _____ Class: _____

Signed: _____ Date: _____

PARENT'S AGREEMENT
I agree to my child having the use of the chromebook on these terms

Signed: _____ Date: _____

HEADTEACHER'S AGREEMENT
I agree on behalf of the school to provide a chromebook on these terms

Signed: _____ Date: _____

Appendix 7

Walking in the footsteps of Jesus with our Christian family, we learn, grow, achieve and flourish together in God's love.

Device loan agreement for pupils

1. This agreement is between:

1) Bretherton Endowed CE Primary School ("the school")

2) Name: _____

Address:_____

("the parent" and "I")

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

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

1. The school is lending the pupil [a chromebook] ("the equipment") for the purpose of [doing schools work from home]

2. This agreement sets the conditions for taking a [Bretherton Endowed CE Primary school chromebook ("the equipment")] home.

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

This home school agreement is applicable for all devices within the 1 to 1 chromebook scheme issued Feb 2022 including one off payments, termed payments over 36 months. All devices remain the property and under the management of Bretherton Endowed for the 3 year term of the insurance and so this agreement remains in place for the full term.

2. Damage/loss

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

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

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

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

I will not leave the equipment unsupervised in unsecured areas.

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

- Keep the device in a secure place when not in use
- Don't leave the device in a car or on show at home
- Don't eat or drink around the device
- Don't lend the device to siblings or friends
- Don't leave the equipment unsupervised in unsecured areas
- To use the recommended case when transporting the device to and from school.

3. Unacceptable use

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

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

This includes, but is not limited to the following:

- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- 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
- Not download apps or software that would be deemed inappropriate based on the child's age and maturity.

I accept that the school will take action, in line with our behaviour policy, if the pupil engages in any of the above **at any time.**

4. Personal use

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

5. Data protection

I agree to take the following measures to keep the data on the device protected.

- Keep the equipment password-protected - strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Make sure my child locks the equipment if it's left inactive for a period of time
- Do not share the equipment among family or friends
- Update antivirus and anti-spyware software as required (Chromebooks operate on a cloud system and so doesn't require additional antivirus)
- Install the latest updates to operating systems, as prompted.

If I need help doing any of the above, I will contact Mrs Carlyon on the email at bursar@bretherton.lancs.sch.uk.

6. Return date

I understand that the device will remain the property of school until the final payment has been made by direct debit. If requested by school, we would ask that you return the device to school office within 3 days of the request.

Depending on the payments made to date, I must inform school if my child is leaving Bretherton Endowed CE Primary school as this may require the device to be returned to school.

7. Consent

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

PUPIL'S FULL NAME	
PARENT'S FULL NAME	
PARENT'S SIGNATURE	

Appendix 8

BRETHERTON ENDOWED CE PRIMARY SCHOOL

Staff ICT Professional Responsibilities

"Walking in the footsteps of Jesus with our Christian family, we learn, grow, achieve and flourish together in God's love."

This policy is for Bretherton Endowed CE Primary School and The Hub, Bretherton Endowed Out of School Provision.

When using any form of ICT, including the internet in school and outside school

For your own protection:

- Ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role.
- Do not talk about your professional role in any capacity when using social media such as Facebook and You Tube
- Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.
- Use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera.
- Do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to pupils, parents, carers and others.
- Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately. This is important for application such as CPOMs.
- Only take images of pupils and/or staff for professional purposes in accordance with school policy and with the knowledge of SLT.
- Do not post any photographs taken at school including children or resources on personal accounts.
- Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Ensure that your online activity, both in school and outside school, will not bring our organisation or professional role into disrepute.
- You have a duty to report any e safety incident whether in or out of school which may impact on you, your professionalism or school.
- This content will be covered by the whistleblowing policy.