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.

This policy has been written as part of the wider policies for Pupil Behaviour, Anti-bullying, Child Protection and Safeguarding; Staff Code of Conduct; Curriculum ; Data Protection.

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; in both administration and curriculum.
- Safe and secure broadband from BT Lancashire including effective management of content filtering and monitoring by school and The ITDept.
- Responsible ICT use by all staff and children, through education and policies
- Equip school staff, governors, 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 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
- Through use of Chromebooks and google learning platform and other IT license applications and software support the school's mission statement and enhance learning across the curriculum in a safe, responsible and transparent way.

- To teach internet safety as named content in our Computing and PHSE curriculum in each year group and celebrated and updated through assemblies (including Internet Safety Day) and others.
- To fulfil our statutory responsibility under KCSiE to provide a safe environment and education where we learn and work, including when online.
- 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

Online Safety details

Designated Safeguarding Lead responsible for Online Safety : Alison Moxham

Deputy DSL _ Jayne Clarke; Sarah Allchurch

Governor responsible for online standards: Laurence Glew

Checklist for compliance :

- Annual and induction online safety training included in safeguarding training for all staff
- ICT code of conduct for all staff and volunteers
- Children and staff acceptable use agreement
- Golden computing rules known by children
- Planned Internet access monitoring and filtering audits each term as part of DSL meeting
- Data collection in line with GDPR principles

Legislation and guidance

The DfE Keeping Children Safe in Education statutory guidance requires Local Authorities, Multi Academy Trusts, and schools in England to ensure learners are safe from harm:

"It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college 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"

"Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college 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"

The DfE Keeping Children Safe in Education guidance also recommends:

Reviewing online safety … Technology, and risks and harms related to it, evolve, and change rapidly. Schools and colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face.

The DfE Keeping Children Safe in Education guidance suggests that:

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

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.

Schools in England are subject to an increased level of scrutiny of their online safety practices by Ofsted Inspectors during inspections, while the Counter Terrorism and Securities Act 2015 requires schools to ensure that children and young people are safe from terrorist and extremist material on the internet.

Roles and responsibilities

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body".

This review will be carried out by the Governing body, led by Online Safety Governor who will receive regular information about online safety incidents and monitoring reports.

The Online Safety Governor responsibilities will include:

- regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by the Headteacher/ DSL,Online Safety Lead, and the Online Safety Governors- in-line with the DfE Filtering and Monitoring Standards
- reporting in governors' meetings
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards- through National Online Safety Platform

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

The DSL (Headteacher) with Deputy DSL's support (Deputy head and Online Safety Lead)

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role supported by the Online Safety Lead and Deputy DSL's.
- have operational responsibility for ensuring development, maintenance and review of Online Safety Policy and associated documents.
- Ensure policy is implemented and compliance with the policy is monitored and accurate records kept.
- Ensure all staff are aware of reporting procedures and requirements in the event of an online safety incident
- Receive relevant and regularly updated training in online safety to enable them to understand the 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
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)
- liase with Safeguarding lead on preventing extremism through safe practise of computing

The Headteacher (Also DSL)

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.

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 monitoring reports.

The Headteacher with The ITDept technical support is responsible for:

- ensuring that 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 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

Online Safety Lead

The Online Safety lead will support with day to day responsibility for online safety.

They will:

- Receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
- Content, contact, conduct and commerce
- Along with the DSL, take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents.
- 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 using Google Forms. **Appendix 3**
- 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.

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 out of school
- must follow and adhere to our 'Computing 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**
- support routine history checks and monitoring of devices as and when necessary
- 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)**

Parents are permitted to take photographs of their own children on school premises but only for their own use.

Parents are made aware that taking a photograph that includes other children could constitute a potential breach of GDPR.

Parents are made aware that uploading images/video of their child alongside other children is not acceptable unless specific permission has been obtained from the other parents.

Our Remote learning Policy is updated regularly in the event of any expectations on schools to teach remotely.

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

Parents are reminded about this responsibility regularly throughout the year.

All staff

All staff are responsible for:

- Having an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- Understanding that online safety is a core part of safeguarding and recieve regular updated training

- 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
- Staff understand that school information/photographs on school devices are not downloaded to personal devices. Staff have permission to take photograph/ video/ audio of children in school but not on personal recording equipment.
- Ensuring that pupils follow the school's terms on acceptable use/ 1-1 device agreement and the golden rules for computing
- 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 .
- All digital communications with learners and parents/carers are on a professional level and only carried out using official school system
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Supervising and monitoring the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- Adhering to parents consent for use of publishing photographs or pupils work in online platforms eg Twitter, Website etc.
- Ensuring there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.
- Maintaining an understanding of this policy and implementing it consistently

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 and sign to confirm understanding annually.

Education & Training – 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 Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings.

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

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.

Educating pupils about online safety

At Bretherton, we believe that while regulation and technical solutions are particularly important, their use must be balanced by educating our pupils to take a responsible approach. The education of our pupils in online safety is therefore an essential part of our online safety

provision. We feel it is vital to help and support children to recognise and avoid online safety risks and develop their resilience.

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for:

"a carefully sequenced RSHE curriculum, based on the Department for Education's (DfE's) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of 'nudes'.."

Keeping Children Safe in Education states:

"*Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college 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 …*"

We ensure that:

- Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum.
- The online safety curriculum is broad, relevant and provide progression, with opportunities for creative activities and will be provided through our explicit Computing and PSHE lessons supported by Jigsaw, Purple Mash and National Online Safety platform (Part of National College). Online safety learning will continue to be threaded through the curriculum. Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learning will make use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week which will be used to reinforce learning, highlight key learning and communicate messages to parents and carers.
- 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.

Educating parents about online safety

The school will raise parents' awareness of internet safety in newsletters 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 and assemblies to mark national online safety events.

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 Online Safety lead.

Contribution of Learners

At Bretherton, we acknowledge, learn from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- Pupil questionnaires to gather learner feedback and opinion.
- Appointment of digital leaders to model good practice and contribute to the online safety programme.
- The Online Safety Group/ Digital Leaders has learner representation
- Learners designing/updating acceptable use agreements/ Computing Golden Rules
- Contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.

Social Networks

Staff must adhere to the Social Media Policy.

Staff are permitted to have social network accounts but it is not acceptable to post content that:

- Brings the school in disrepute
- Leads to parental complaints
- Deemed derogatory towards school or employees
- Deemed derogatory towards pupils, carers or parents
- Brings into question their ability to work with children

Staff social media accounts should be 'Private' and not open to public scrutiny.

It is not acceptable for staff to accept friend requests from students currently enrolled in school unless they are family members.

Communication with past pupils , parents or siblings of pupils not in school is discouraged

Parents should be aware that posting inappropriate comments about individual members of staff or children could be construed as online bullying

It is not acceptable for parents to discuss issues that they may be experiencing at school on social media as it may bring the school into disrepute.

Parents are made aware of the legal age requirement for social media profiles is 13 years of age

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.)

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 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.

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.

Preventing Extremism

The school is aware that it has a role to play to prevent radicalisation and extremism. To prevent the radicalisation of young people, the school will

- Have a filtering system to block out inappropriate websites
- A reporting system (CPOMS) to keep a record of any incidents that occur and will refer any concerns through the Channel programme or if appropriate the Police.
- Fulfil training responsibilities for all staff, Governors and parents
- Has acceptable user policies in place for all stakeholders
- Through education, children know what is acceptable or not even though the filters are in place.

E-mail

All staff have access to Office 365 for work based emails. Staff are permitted to access personal emails on school premises or on school equipment at non teaching times where no children are present.

Only official email accounts are to be used for professional communication.Any spam or virus on official e-mail accounts should be reported to the HT

Access to technology

When accessing online material, children are supervised by a trusted adult and protected by the online filtering system

Children have access to their own 'Drive and classroom and content is restricted. They do not have unrestricted access to other areas of the server. Confidential information is retained on the office server eg SIMS with limited staff access

All users of the school network have secure username and password. The admin for the network lies with The ITDept, HT and Bursar. It is stored in a safe location

Technology

The DfE Filtering and Monitoring Standards states that "Your IT service provider may be a staff technician or an external service provider". If the school has an external technology provider, it is the responsibility of the school to ensure that the provider carries out all the online safety and security measures that would otherwise be the responsibility of the school. It is also important that the technology provider is fully aware of the school Online Safety Policy/acceptable use agreements and the school has a Data Processing Agreement in place with them. The school should also check their local authority/other relevant body policies on these technical and data protection issues if the service is not provided by the authority and will need to ensure that they have completed a Data Protection Impact Assessment (DPIA) for this contract.

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Our school uses Netsweeper as its internet filtering system provided by BT Lancashire and Sophos antivirus software. The school completes regular filtering checks through The ITDept to ensure that subjects linked to child abuse and terrorist content in blocked.

Critical updates are completed by school technician with high level of expertise.

The DSL and Online Safety Lead check weekly reports to ensure appropriate use , report to Governors on a termly basis. Any breaches will be dealt with in accordance with our safer use expectations.

Online safety incidents and breaches form part of our termly DSL meetings.

Filtering & Monitoring

The DfE guidance (for England) on filtering and monitoring in "Keeping Children Safe in Education" states:

"It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place …governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the … risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team 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…

The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards…"

The school's filtering and monitoring provision(Netsweeper) is agreed by senior leaders, governors and the IT Service Provider, The ITDept and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL (along with the Online Safety Lead) will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility.

The filtering and monitoring provision is reviewed annually by the Head/ the Designated Safeguarding Lead, the Online Safety Governor with the involvement of the IT Service Provider.

Checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of the Headteacher/Designated Safeguarding Lead, Online Safety Lead and Online Safety Governor , in particular when a safeguarding risk is identified, there is a change in working practice.

Monitoring

We have **monitoring systems in place to protect the school, systems and users:**

- The school monitors all network use across all its devices and services.
- Monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead and Online Safety Lead. All users are aware that the network (and devices) are monitored.

- There are effective protocols in place to report abuse/misuse.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- Staff physically monitor and supervise devices being used in the classroom.
- Half-termly more in depth random spot checks are carried out on pupil devices, finding logged and any breaches reported and dealt with through our online safety breach forms.
- Filtering logs are regularly analysed and breaches are reported to senior leaders
- Pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.

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 9**). 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 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
- 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 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 safe guarding issues should be reported to DSL immediately and will be followed using the right hand side of the flow chart.

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 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.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety that has been reported through CPOMS from the Online Safety Reporting Forms.

This policy will be reviewed every year by the Computing subject leader.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour 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
- Twitter policy

Written by- S. Allchurch- Online safety lead

Adopted : Sept 25
To be reviewed by the end of 2027

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

Appendix 1: Monitoring and Filtering Policy

Appendix 2: Who is responsible for tech security
Appendix 3 Access Rights
Appendix 4: Monitor reports
Appendix 5: Guest access
Appendix 6: Data Handling
Appendix 7: Events Log
Appendix 8: Flow chart of reporting
Appendix 9: Online Safety Reporting Form
Appendix 10: Computing Golden Rules
Appendix 11: Online Reporting Button
Appendix 12: Home school agreement
Appendix 13: 1 to 1 Device agreement
Appendix 14 : Professional ICT Responsibility agreement
Appendix 15: Acceptable use agreements – pupil and staff and volunteers

Apendix 1

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 : March 2025

To be reviewed :No later than the end of 2027

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

Appendix 1 cont …

Appropriate secutity measures are in place 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 through:

- Height of hardware
- Lockage cabinet
- Password protected sites
- Security of passwords in place
- Policy for personal data equipment

Appendix 2

Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff

Overall security manager: Head teacher
Second : Online Safety Governor
Support in school through bought in service: IT Solutions. Matthew Schofield
Local Authority support/advice: BTLS Lancashire

Appendix 3 –

Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually.

Access Rights	Name
Administrator	Headteacher
	Matt Schofield
Staff rights	All school staff including Bursar
Children	Restricted rights

Appendix 4:

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.

Date	*Random audit of use involving:*	*Outcomes/action*

5:1 An appropriate system is in place for users to report any actual / potential technical incident to the Online Safety Coordinator

On identification of an actual/potential technical incident, the informant must report to Head teacher using the potential breach form (See Online Safety Policy)

Incidents involving adults

- Close computer if appropriate
- Pass information toHeadteacher, DHT or school office using reporting form
- Head teacher to follow protocol in Online safety policy

Incidents involving children

- Establish the facts and close the computer without deleting/ closing the package
- Remove the computer and child from the area
- Pass the computer to the Headteacher to ascertain the facts for reporting
- Speak to child and support as required, reminding them of safeguarding responsibilities
- Contact parents
- Complete safeguarding incident report for accurate reporting to governors
- Depending on the severity of incident, contact online safety governor

Appendix 5

6:1 An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system

- Log in for guests/ students will be provided.
- Only 1 guest user name and password will be used at any time and diary entry of who using to support investigation of possible future breach
- Additional monitoring may be required at periods of additional guests/visitors using our network
- Guest internet log in supports additional filtering/ monitoring should we require it.

6:2 An agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users

- Staff should not download any files or programmes that are saved onto the school server. Minor files can be downloaded and saved onto individual computers, however if in any doubt as to the validity of the programmes, advice MUST be sought.

6:3 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.

Appendix 6

An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. (see School Personal Data Policy Template in the appendix for further detail)

School Personal Data Handling Policy

Introduction

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office - for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

The DPA lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and correction. The DPA requires organisations to comply with eight data protection principles, which, among others require

Commissioner's Office website:
http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx

Policy Statements

The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including children, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, children progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

Responsibilities

The school's Senior Information Risk Officer (SIRO) is the Head Teacher. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The school will identify Information Asset Owners (IAOs) -School business officers for the various types of data being held (e.g. pupil / student information / staff information / assessment data etc.). The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose.
- how information as been amended or added to over time, and
- who has access to protected data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.
http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx

Information to Parents / Carers – the "Privacy Notice"

In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all pupils / students of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents / carers through display in entrance hall and on school website. Parents / carers of young people who are new to the school will be provided with the privacy notice through their welcome pack.

Training & awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through: Induction training for new staff

- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners

Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

Risk ID	Information Asset affected	Information Asset Owner	Protective Marking (Impact Level)	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

Impact Levels and protective marking

Government Protective Marking Scheme label	Impact Level (IL)	Applies to schools?
Not Protectively Marked	0	Will apply in schools
Protect	1 or 2 mostly in schools	
Restricted	3	
Confidential	4	Will not apply in schools
Highly Confidential	5	
Top Secret	6	

The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts students / pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer e.g.. "Securely delete or shred this information when you have finished using it".

Secure Storage of and access to data

The school will ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords which must be changed regularly.User passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media. Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected,
- the device must be password protected
- the device must offer approved virus and malware checking software, and
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

The school has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example dropbox, Microsoft 365, google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

As a Data Controller, the school is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

The school recognises that under Section 7 of the DPA, http://www.legislation.gov.uk/ukpga/1998/29/section/7 data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform;
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;

- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation. A destruction log is kept in school office.

Audit Logging / Reporting / Incident Handling

It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by responsible individuals.

The audit logs will be kept to provide evidence of accidental or deliberate_data security breaches – including loss of protected data or breaches of an acceptable use policy, for example.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident;
- a communications plan, including escalation procedures;
- and results in a plan of action for rapid resolution; and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Use of technologies and Protective Marking

The following provides a useful guide:

	The information	The technology	Notes on Protect Markings (Impact Level)
School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events	Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning and achievement	Individual pupil / student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be students/ pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this pupil / student record available in this way.
Messages and alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send

	when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information, or be used to provide further detail and context.	detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

Appendices: Additional issues / documents related to Personal Data Handling in Schools:

Use of Biometric Information

Parental permission for use of cloud hosted services

Currently Bretherton doesn't operate a cloud based system.

Schools that use cloud hosting services (eg.Google Aps for Education) may be required to seek parental permission to set up an account for pupils / students.

Google Apps for Education services - http://www.google.com/apps/intl/en/terms/education_terms.html requires a school to obtain 'verifiable parental consent'. Normally, schools will incorporate this into their standard acceptable use consent forms sent to parents each year (see suggested wording on "Parent / Carer Acceptable Use Agreement Template").

A template form has been added to the Parents & Carers Acceptable User Template elsewhere in these Template Policies.

Privacy and Electronic Communications

Schools should be aware that they are subject to the Privacy and Electronic Communications Regulations in the operation of their websites.

Freedom of Information Act

All schools (including Academies, which were previously exempt) must have a Freedom of Information Policy which sets out how it will deal with FOI requests. In this policy the school should:

- Delegate to the Headteacher / Principal day-to-day responsibility for FOIA policy and the provision of advice, guidance, publicity and interpretation of the school's policy
- Consider designating an individual with responsibility for FOIA, to provide a single point of reference, coordinate FOIA and related policies and procedures, take a view on possibly sensitive areas and consider what information and training staff may need
- Consider arrangements for overseeing access to information and delegation to the appropriate governing body
- Proactively publish information with details of how it can be accessed through a Publication Scheme (see Model Publication Scheme below) and review this annually

- Ensure that a well-managed records management and information system exists in order to comply with requests
- Ensure a record of refusals and reasons for refusals is kept, allowing the Academy Trust to review its access policy on an annual basis

Model Publication Scheme

The Information Commissioners Office provides schools and academies with a model publication scheme which they should complete. This was revised in 2009, so any school with a scheme published prior to then should review this as a matter of urgency. The school's publication scheme should be reviewed annually. (see separate Model Publication Scheme)

Appendix - DfE Guidance on the wording of the Privacy Notice

Bretherton Endowed CE Primary School

Privacy Notice - Data Protection Act 1998

We Bretheton Endowed CE Primary School are a data controller for the purposes of the Data Protection Act. We collect information from you and may receive information about you from your previous school and the Learning Records Service. We hold this personal data and use it to:

- Support your teaching and learning;
- Monitor and report on your progress;
- Provide appropriate pastoral care, and
- Assess how well your school is doing.

This information includes your contact details, national curriculum assessment results, attendance information and personal characteristics such as your ethnic group, any special educational needs and relevant medical information. If you are enrolling for post 14 qualifications we will be provided with your unique learner number (ULN) by the Learning Records Service and may also obtain from them details of any learning or qualifications you have undertaken.

We will not give information about you to anyone outside the school without your consent unless the law and our rules allow us to.

We are required by law to pass some information about you to the Local Authority and the Department for Education (DfE)

If you want to see a copy of the information about you that we hold and/or share, please contact the school office.

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites: http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause

If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

Public Communications Unit, Department for Education
Sanctuary Buildings
Great Smith Street
London
SW1P 3BT

Website: www.education.gov.uk

Email: http://www.education.gov.uk/help/contactus
Telephone: 0370 000 2288

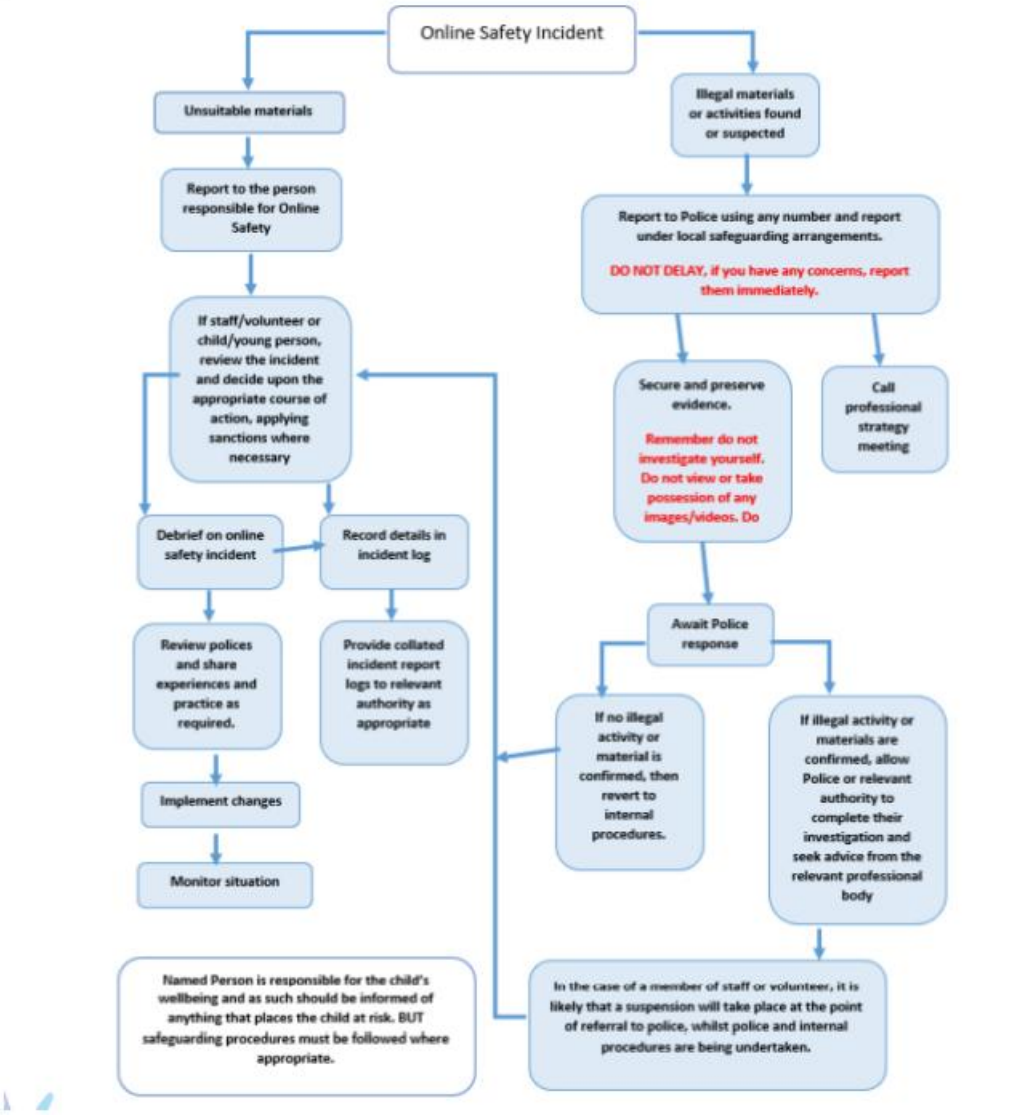
Appendix 7

Events log

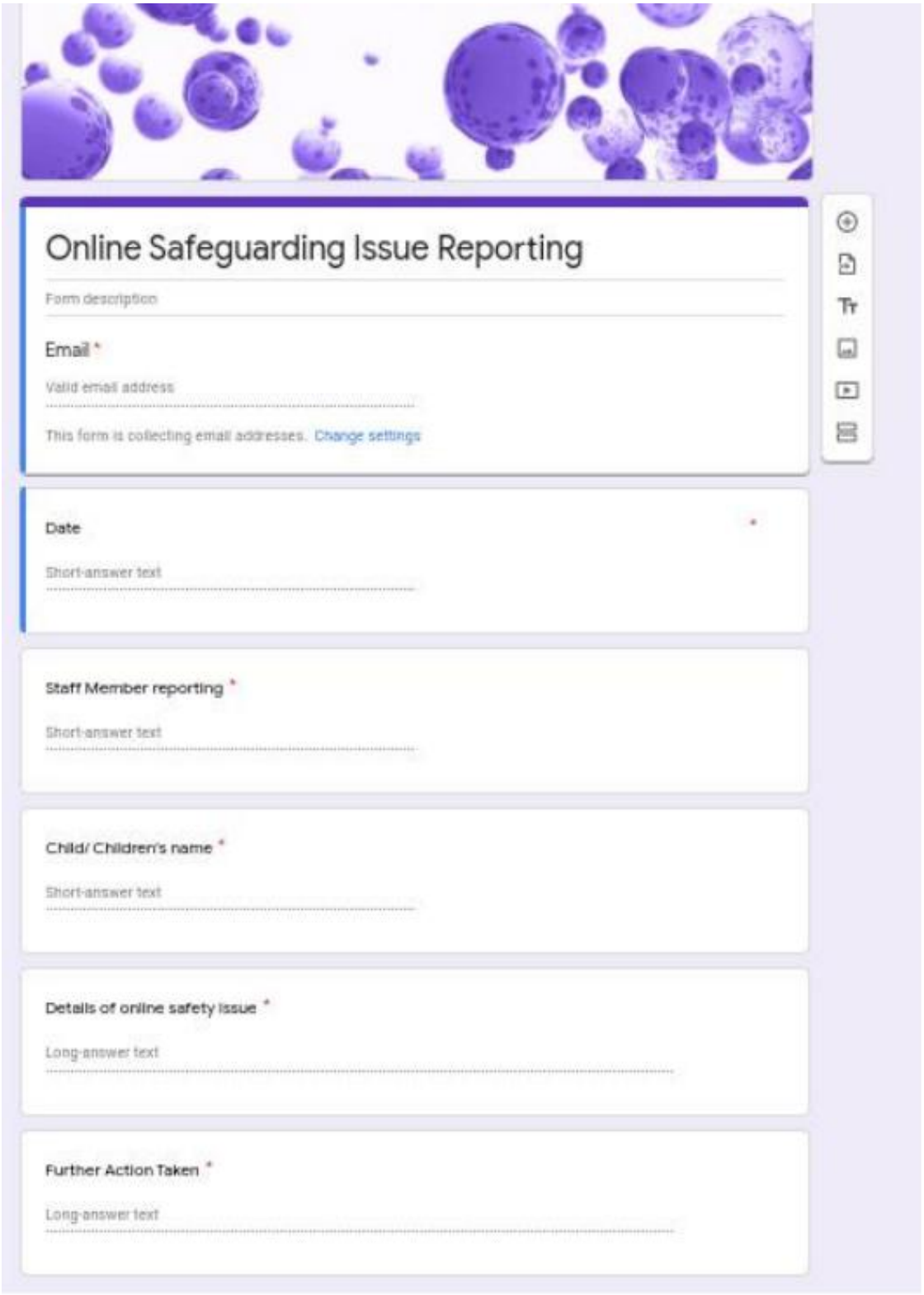
Date	Staff	Event description	Comments	Signed off

Appendix 8: Flow chart of reporting

Appendix 2 Reporting internet misuse or online safety breeches



Appendix 9: Online Safety Reporting Form



Online Safeguarding Issue Reporting

Form description

Email *

Valid email address

This form is collecting email addresses. Change settings

Date *

Short-answer text

Staff Member reporting *

Short-answer text

Child/ Children's name *

Short-answer text

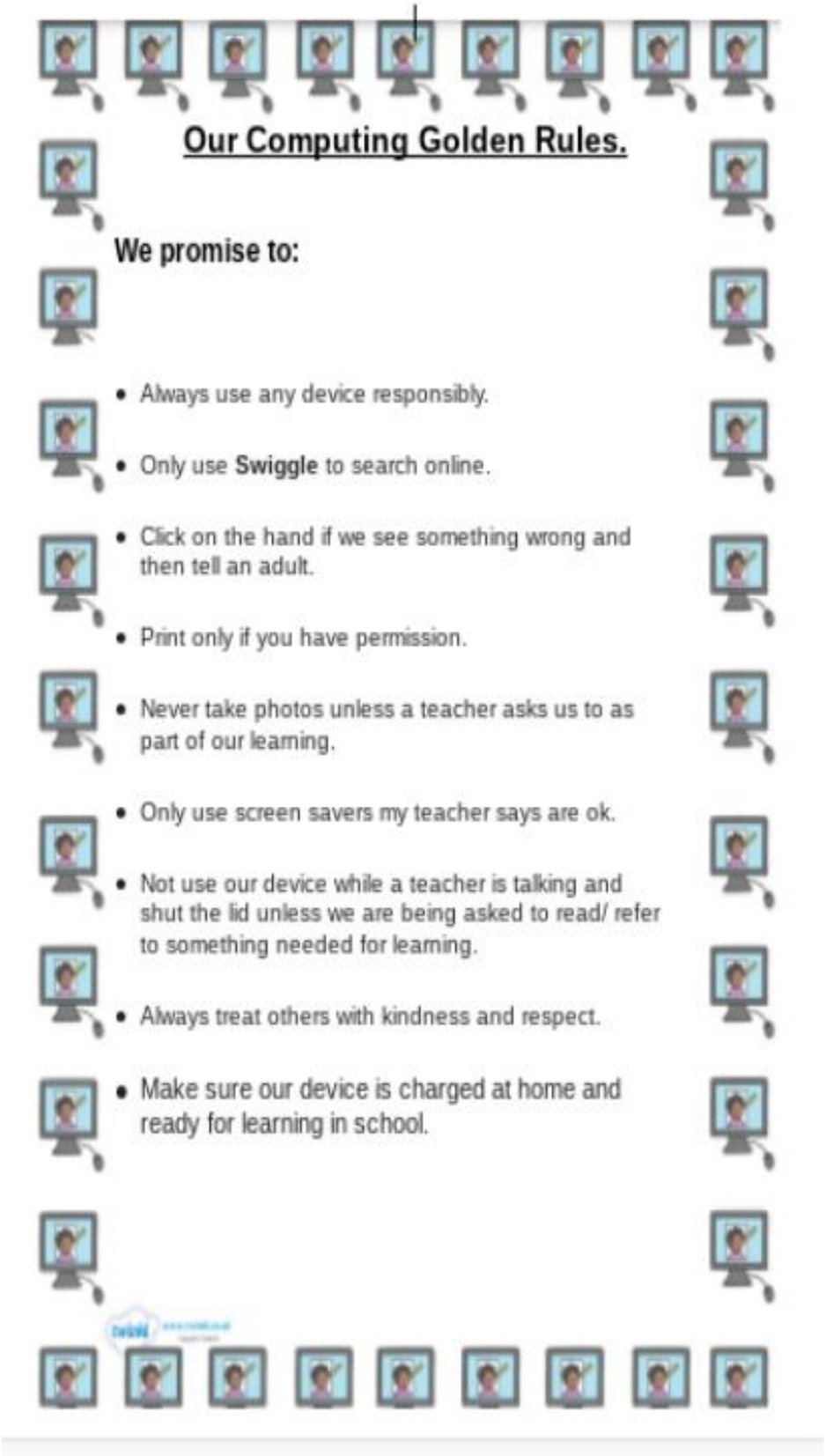
Details of online safety issue *

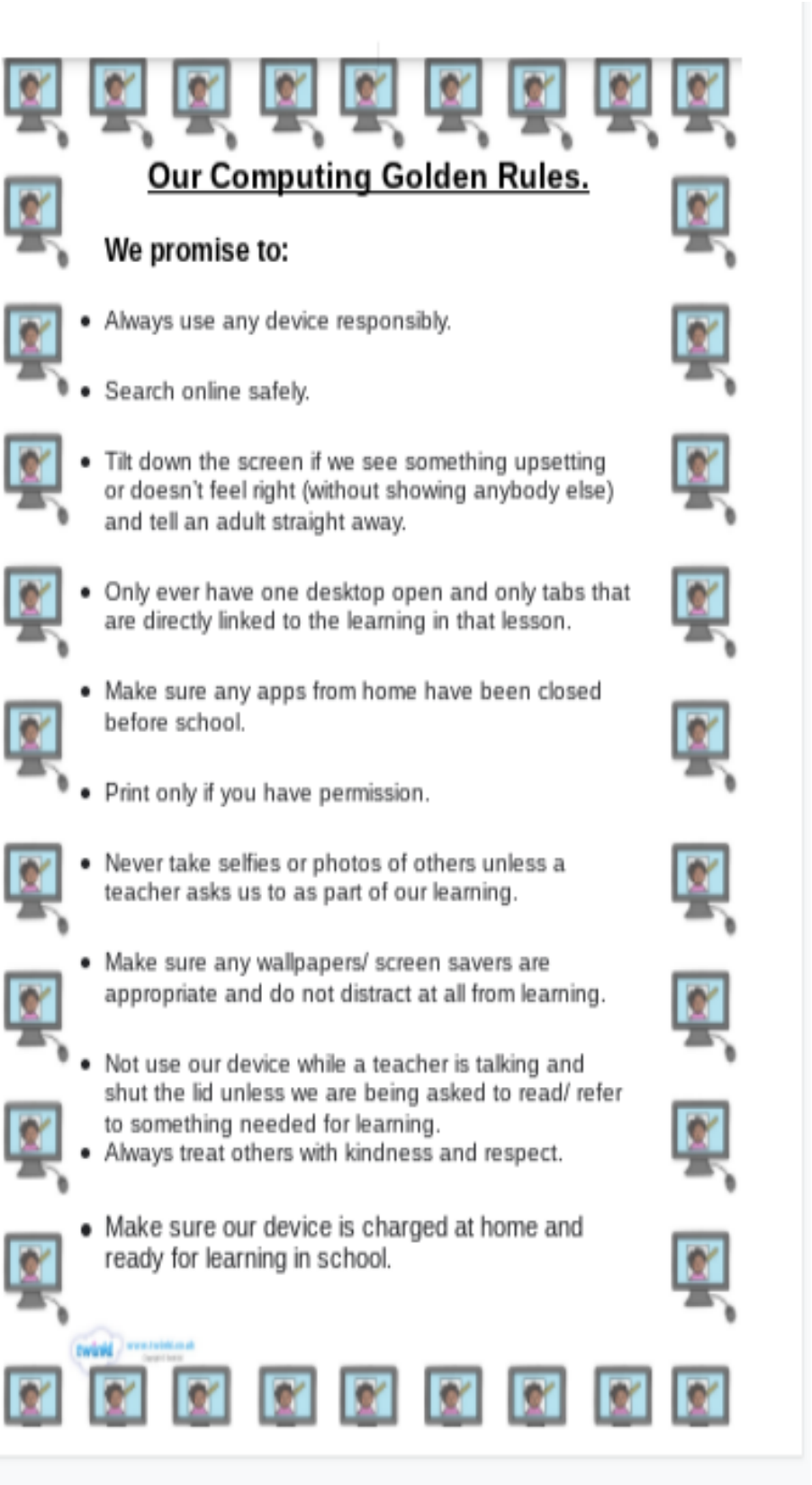
Long-answer text

Further Action Taken *

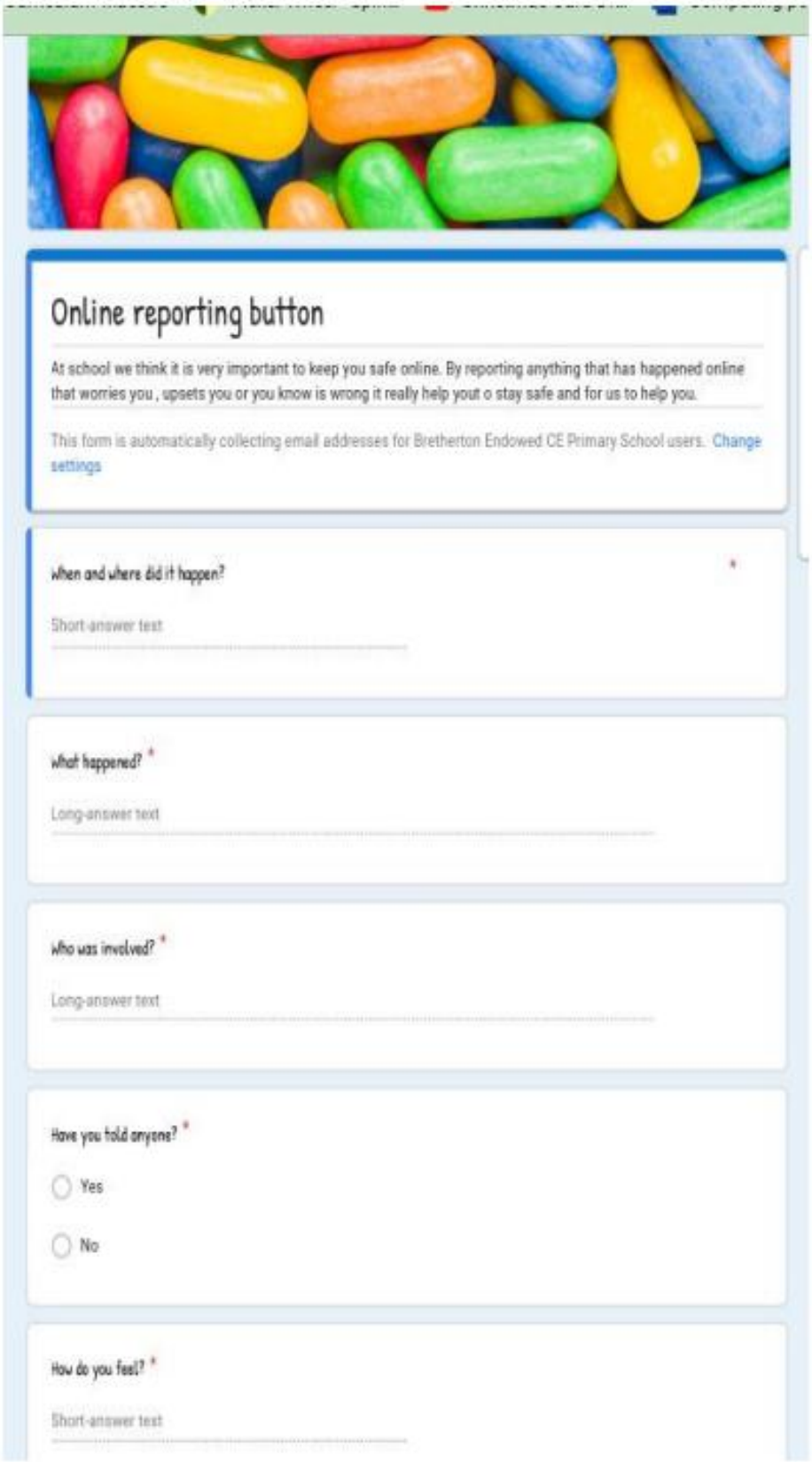
Long-answer text

Appendix 10: Computing 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 11: Online Reporting Button



Online reporting button

At school we think it is very important to keep you safe online. By reporting anything that has happened online that worries you , upsets you or you know is wrong it really help yout o stay safe and for us to help you.

This form is automatically collecting email addresses for Bretherton Endowed CE Primary School users. Change settings

when and where did it happen? *

Short-answer text

what happened? *

Long-answer text

who was involved? *

Long-answer text

Have you told anyone? *

- Yes
- No

How do you feel? *

Short-answer text

Appendix 12: Home school agreement

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 13: 1 to 1 Device agreement

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 14: Professional ICT Responsibility agreement

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.

Appendix 15 : Acceptable use agreements – pupil and staff and volunteers
See website