Baldwins Gate CE Primary School

Online Safety Policy

Date of review	January 2022
Chair of Governors	Fiona Boulton
Headteacher	Leanne Lowndes
Date of next review	January 2024

The School is committed to safeguarding and promoting the welfare of children and expects all staff and volunteers to share this commitment.

Baldwins Gate CE (VC) Primary School
Online Safety Policy

Principles and Values
Baldwins Gate CE Primary School is a Christian school where everyone can learn about their own self-worth in a caring atmosphere of respect, tolerance and co-operation. We intend this to be a happy place where children feel valued. We encourage our children to be independent, confident learners, able to make positive contributions for themselves and others.

Our vision statement
Baldwins Gate Primary School is a Christian school where children, inspired by our Christian values, learn together to be the best that they can be.

Through respect, tolerance, and kindness they learn that they are unique and valued and to celebrate the value and uniqueness of others.

> *Love is patient, love is kind.*
> *It always protects, always trusts, always perseveres.*
> *Corinthians 13*

Our mission statement:
Everyone learning together in faith, truth and love

This policy
Baldwins Gate CE VC Primary school recognises that ICT and the internet are effective tools for learning and communication that can be used in school to enhance the curriculum, challenge pupils, and support creativity and independence.

This policy aims to be an aid in regulating online activity in school and provide a good understanding of appropriate use. Online safety is a whole-school issue and responsibility. Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures which are outlined in our behaviour policy.

Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good online safety.

It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

Online safety covers the internet but it also covers mobile phones and other electronic communications technologies.

We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings.

There is a ‘duty of care’ for any persons working with children and educating all members of the school community on the risks and responsibilities of online safety falls under this duty. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential.

A Positive Approach to Online Safety
Online safety for children is an important topic and should be addressed and approached with a positive and welcoming mindset. Digital technologies are creating the world around us and we must all take responsibility to educate and help children safely navigate the digital space.
If we do this successfully, our children will be free to learn and experience more than many of us could ever have imagined.

Open, Honest Conversation
Keeping children safe online is all about openness and honesty. Conversations about online safety should engage young people on the topics of interest to them, whether that may be social media, gaming, chatting, or browsing and learning, as well as giving support, guidance and advice on how to behave and report content if needed.

If you can focus on these three key principles, you will find your conversations about online safety are well-received and have a lasting effect.

Trust
Make sure our children or the young people you are speaking with feel trusted. If you do not, you will quickly find any conversations you have about being online become defensive and protective, creating an environment of privacy, uncertainty, and silence.

Positivity
The internet is incredible. Jaw-droppingly, mind-blowingly, world-changingly amazing. The potential it holds is unfathomable and it can enrich our lives in ways that were never possible for humankind before 1990. The benefits of being online far outweigh the risks.

Empowerment
By giving young people the tools and strategies to navigate their online experience safely, you will empower them to achieve and discover more. When we practice online safety, we unlock great potential in ourselves and the people with whom we interact.

Development/Monitoring/Review of this Policy
This online safety policy has been developed by a working group/committee made up of:

- Headteacher and senior leaders
- Staff – including teachers, support staff, technical staff
- Governing Board
- Parents and carers
- Community users

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Surveys/questionnaires of
    - pupils
    - parents/carers
    - staff

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of

staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying/cyber-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Roles and Responsibilities

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

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by link governors or through the online safety committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Board has taken on the role of Online Safety Governor. This role is combined with that of the Child Protection/Safeguarding Governor.

The role of the Online Safety Governor includes:

- regular meetings with the Online Safety Co-ordinator
- attendance at Online Safety committee meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors/Board Committee and Full GB meetings.

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community,
- The school has a designated Online Safety Lead. This is Mrs Stephanie Maude. She is also the Designated Safeguarding Lead for the school.
- The Headteacher and SALT and Computing lead should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority and school disciplinary procedures).
- The Headteacher and Senior Leaders are responsible for ensuring that relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with Local Authority
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with the Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of *Governors*
- reports regularly to Senior Leadership Team
- any reported incidences will be dealt with in line with the staff code of conduct

Network Manager/Technical staff

Those with technical responsibilities are responsible for ensuring:

- **that the school's technical infrastructure is secure and is not open to misuse or malicious attack**
- **that the school meets required online safety technical requirements and any Local Authority and relevant Board online safety policy/guidance that may apply.**
- **that users may only access the networks and devices through a properly enforced password protection policy**
- **the school's filtering system is currently Surf-Protect by Exa Networks.**
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Senior Leaders and Online Safety Lead for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- **They have an up-to-date awareness of online safety matters and of the current school online safety policy and practices**
- **They have read, understood and signed the staff acceptable use policy/agreement (AUP/AUA)**
- **They report any suspected misuse or problem to the Headteacher/Senior Leader/Online Safety Lead) for investigation/action/sanction**
- **All digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems**
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the E safety/Online Safety Policy and acceptable use policies
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

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

Designated Safeguarding Lead
Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

(NB it is important to emphasise that these are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop.)

Online Safety Committee
The Online Safety Committee provides a consultative forum that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring of the Online Safety Policy including the impact of initiatives. The committee will also be responsible for regular reporting to the Governing Board.

Members of the Online Safety Committee will assist the Online Safety Lead (or other relevant person, as above) with:

- the production/review/monitoring of the school online safety policy/documents.
- mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/filtering/incident logs
- consulting stakeholders – including parents/carers and the pupils about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool

Pupils:

- **Are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement at an age-appropriate level**
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies, at an age-appropriate level on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying/cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's/academy's online safety policy covers their actions out of school, if related to their membership of the school

Parents/carers
Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website

Community Users
Community Users who access school systems or programmes as part of the wider school provision will be expected to agree to our school's Acceptable Use Policy before being provided with access to school systems.

Policy Statements

Education – Pupils
Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

In planning their online safety curriculum we refer to:

- DfE Teaching Online Safety in Schools
- Education for a Connected Word Framework
- South West Grid For Learning (SWGf) Project Evolve – online safety curriculum programme and resources

Through the Evolve Project children at Baldwins Gate learn about and practise the 8 domains of good online safety habits. They learn about these areas through PSHE and Computing. The teaching of all domains are supported in a variety of subjects and special online safety days. The 8 domains and where they are taught are detailed below.

Evolve Project Online Safety Teaching Domains

PSHE	Computing
Self-Imagine and Identity	Copyright and Ownership
Online Relationships	Management and Ownership
Online Reputation	Privacy and Security
Online Bullying	
Health and Wellbeing and Lifestyle	

For further information about these areas please see relevant curriculum statements and policies.

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 should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:-

A planned online safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited

- **Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities**
- **Pupils should 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 should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.**
- **Pupils should 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.** Schools have additional duties under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- Pupils should be helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Pupils should be provided with the opportunity to explore our online safety, child friendly version of our online safety policy.

Education – Parents/carers

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

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents/carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers

Education & Training – Staff/Volunteers/Governors

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 (or other nominated person) will receive updates through attendance at external training events, online safety newsletters, Staffordshire Safeguarding Board updates and by reviewing guidance documents released by relevant organisations as required.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.

Training – Governors

Governors take receive online safety information posters and are given the opportunity to attend training or an awareness raising sessions.

This may be offered in a number of ways:

- Participation in school training/information sessions for staff or parents and or workshops
- External partner training.

Technical – infrastructure/equipment, filtering and monitoring

The school in conjunction with the IT provider 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. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All staff will have clearly defined access rights to school technical systems and devices.** Children share log ins, but iPad numbers are noted to certain children.
- **All pupils are provided with a username and password.** The school's aim is to begin providing children in at least Key Stage Two with their own log in, usernames and passwords. **Users are responsible for the security of their username and password**. Where appropriate we may choose to use group or class logons and passwords for Key Stage 1 and EYFS pupils, but the school should constantly consider and evaluate whether this models good password practice and need to be aware of the associated risks.
- The "master/administrator" passwords for the school systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g., school safe)
- The school office 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 as inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs

- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- **Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.** The school recognises that they have additional duties under the Counter Terrorism and Securities Act 2015 (PREVENT) which requires us to ensure that children are safe from terrorist and extremist material on the internet.
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc).
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- An appropriate system/s is in place to report any actual/potential technical incident/security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up-to-date virus software.
- An agreed protocol is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed protocol is in place which is described in the staff code of conduct/ staff behaviour policy regarding the extent of personal use that users (staff/pupils/community users) and their family members are allowed on school devices that may be used out of school. *that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.*
- An agreed policy is in place (Acceptable Use Policy) regarding the use of removable media (e.g., memory sticks/CDs/DVDs) by users on school devices. **Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.**

To ensure an effective and appropriate monitoring procedure at Baldwins Gate we operate a pro- active and active approach to monitoring.

Proactive Monitoring- Children are constantly monitored by the class teacher and school staff as they walk around the room. * (2022 the schools aim is to develop our proactive monitoring systems further).

Active Monitoring- The schools surf-protect sends daily updates that monitor and indicates where school devices have tried to connect to inappropriate content. This is then dealt with following the schools' appropriate channels.

Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy is consistent with and inter-related to

other relevant school polices including but not limited to the safeguarding policy, behaviour policy, anti-bullying policy, cyber-bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's online safety education programme.

In preparing a mobile technologies protocol the school has considered the possible issues and risks. These include: security risks in allowing connections to the school network, filtering of personal devices, breakages and insurance, access to devices for all students, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership. Such matters are also included in the school's Acceptable Use Policy

- **The school acceptable use agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies.**
- **The school allows the following:**

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Pupil owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*No**	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*		*No*	*No*
Internet only					*Yes*	*Yes*
No network access						

***Unless where medical conditions require it, this will be looked at and reviewed on a case-by-case basis.**

We have considered the following regarding School owned/provided devices:

- *Who they will be allocated to*
- *Where, when and how their use is allowed – times/places/in school/out of school*
- *If personal use is allowed*
- *Levels of access to networks/internet (as above)*
- *Management of devices/installation of apps/changing of settings/monitoring*
- *Network/broadband capacity*
- *Technical support*
- *Filtering of devices*
- *Access to cloud services*
- *Data Protection*
- *Taking/storage/use of images*
- *Exit processes – what happens to devices/software/apps/stored data if user leaves the school*
- *Liability for damage*
- *Staff training*

Personal devices:

- Which users are allowed to use personal mobile devices in school (staff/pupils/students/visitors)
- Restrictions on where, when and how they may be used in school
- Storage
- Whether staff will be allowed to use personal devices for school business
- Levels of access to networks/internet (as above)
- Network/broadband capacity
- Technical support (this may be a clear statement that no technical support is available)
- Filtering of the internet connection to these devices
- Data Protection
- The right to take, examine and search users devices in the case of misuse (England only) – N.B. this must also be included in the Behaviour Policy.
- Taking/storage/use of images
- Liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility).
- Identification/labelling of personal devices
- How visitors will be informed about school requirements
- How education about the safe and responsible use of mobile devices is included in the school online safety education programmes.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying/cyber-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees in line with the proposals for KCSIE 2022 The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm-

- **When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.**
- **Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press**
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *pupils* in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students'/Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's/Pupil's work can only be published with the permission of the student/pupil and parents or carers.

Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR). As a result, schools are likely to be subject to greater scrutiny in their care and use of personal data. More detailed guidance is available in the GDPR policy document.

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school ensures

- **it has a Data Protection Policy.**
- **it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.**
- **it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).**
- **it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.** In addition, the school has the support of a Data Manager and Systems Controllers to support the DPO
- **it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it**
- **the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded**
- it will hold only 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. The school should develop and implement a 'retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- it provides all with information about how the school looks after their data and what their rights are in a clear Privacy Notice which is provided for staff and parents.
- Procedures are in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- **It has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.**

- **It understands how to share data lawfully and safely with other relevant data controllers.**
- **it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.**
- **As we are a maintained school we have a Freedom of Information Policy which sets out how it will deal with FOI requests.**
- **all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.**

When personal data is stored on any mobile device or removable media the:

- **data must be encrypted and password protected.**
- **Devices that must be password protected include laptops and school iPads.**
- **device must be protected by up to date virus and malware checking software**
- **data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.**

Staff must 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**
- **can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school**
- **where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.**
- **will not transfer any school personal data to personal devices except as in line with school policy**
- **access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data**

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff & other adults			Pupils				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school	■						■	
Use of mobile phones in lessons								■
Use of mobile phones in social time	■							■
Taking photos on personal mobile phones/cameras								■
Use of other mobile devices e.g. tablets, gaming devices	■						■	
Use of personal email addresses in school, or on school network								■
Use of school email for personal emails								■
Use of messaging apps								■
Use of personal social media								■
Use of blogs		■					■	

When using communication technologies, Baldwins Gate CE (VC) Primary School considers the following as good practise;

- **The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.** Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g., by remote access).
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
- **Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content.** These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

- Pupils are taught about online safety issues, such as the risks attached to the sharing of personal details. They are also taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity
All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. All could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render us or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:
- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:
- No reference should be made in social media to pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school /academy* or local authority/MAT
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:
- *A process for approval by senior leaders*
- *Clear processes for the administration and monitoring of these accounts – involving at least two members of staff*
- *A code of behaviour for users of the accounts, including*
- *Systems for reporting and dealing with abuse and misuse*
- *Understanding of how incidents may be dealt with under school disciplinary procedures*

Personal Use:
- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

Monitoring of Public social media:
- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The school's use of social media for professional purposes will be checked regularly by the headteacher who will report to the Online Safety committee to ensure compliance with the school policies. Support and help for school staff is available from their unions or by contacting Professional Online Safety Helpline (0344 381 4772 or helpline@saferinternet.org.uk), which is a free and independent helpline for teachers and others working with children in the UK. If you are aware of content that you do not think should be on social media platforms such as TikTok, then your best route is to call or email the POSH helpline. The POSH helpline team will then report the content directly to the teams working on these issue, who can take action.

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

At Baldwins Gate we are aware of the 4 C's of online safety as define by KCSIE 2021. Staff are aware of how these areas affect children online and consideration to these 4 areas has been given when developing this policy. These 4 areas of risk are detailed below;

1. Content
   'Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism' (KCSIE 2021).

2. Contact
   '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' (KCSIE 2021).

3. Conduct
   'Conduct: personal 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' (KCSIE 2021).

4. Commerce
   'Commerce – risks such as online gambling, inappropriate advertising, phishing and or financial scams' (KCSIE 2021).

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				X	
On-line gaming (educational)	X	X			
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping/commerce				X	
File sharing				X	
Use of social media				X	
Use of messaging apps				X	
Use of video broadcasting e.g. Youtube			X		

Responding to incidents of misuse

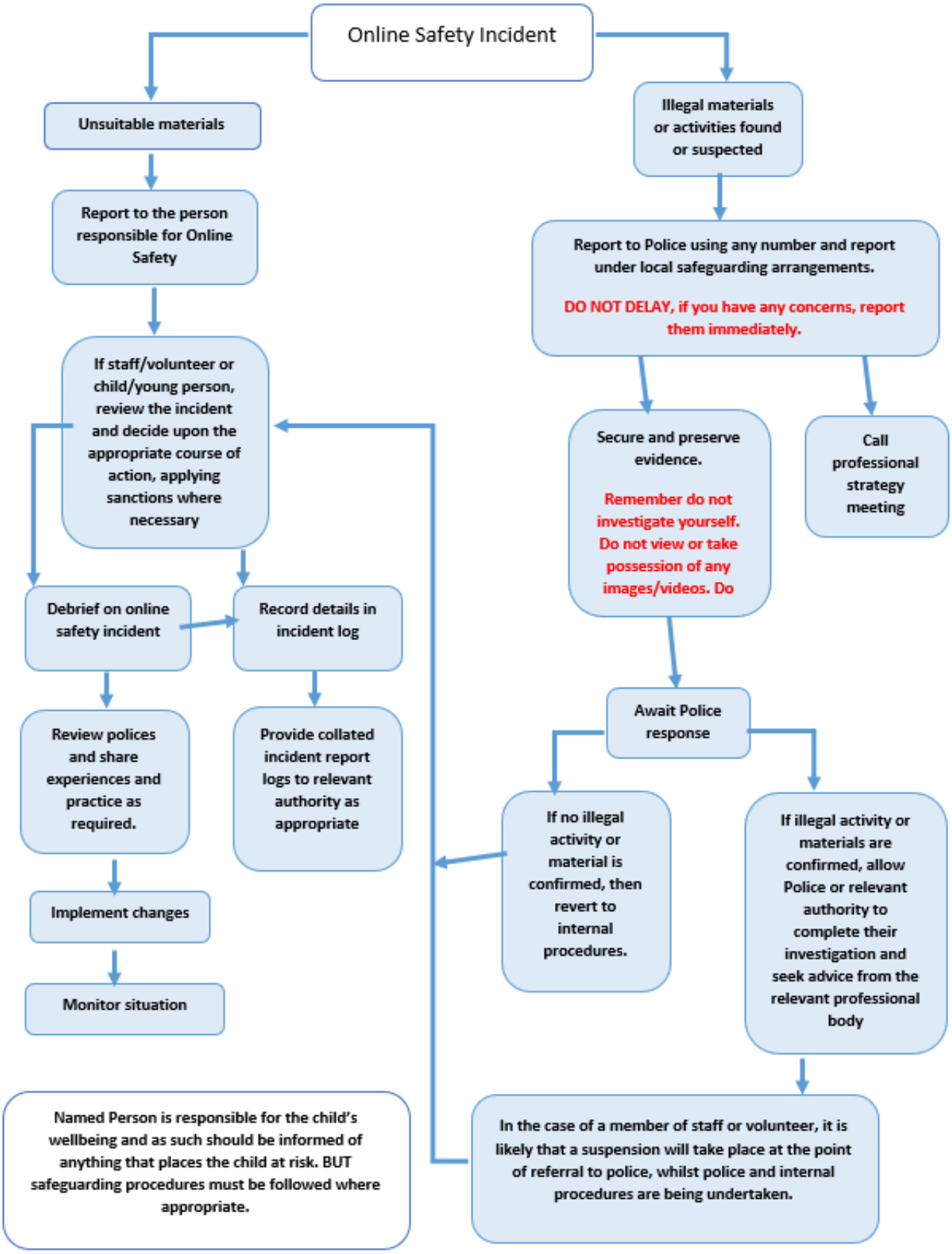
It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:
If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the contact the Staffordshire Safeguarding Children's Board.

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

If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or material

The following flow chart supports the school in how to respond to an incident of misuse



Sanctions for misuse

Pupils	Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering /	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	√	√	√	√	√	√	√	√	√
Unauthorised use of non-educational sites during lessons	√				√		√	√	
Unauthorised use of mobile phone / digital camera / other handheld device	√		√			√		√	
Unauthorised use of social networking / instant messaging / personal email	√		√		√	√	√	√	
Unauthorised downloading or uploading of files	√		√		√		√	√	
Allowing others to access school network by sharing username and passwords	√				√			√	
Attempting to access or accessing the school network, using another student's / pupil's account	√				√		√	√	
Attempting to access or accessing the school network, using the account of a member of staff	√		√		√	√	√	√	
Corrupting or destroying the data of other users	√							√	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	√		√		√	√	√	√	
Continued infringements of the above, following previous warnings or sanctions	√		√			√			√
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	√		√			√	√		√
Using proxy sites or other means to subvert the school's filtering system	√		√	√	√	√	√		√
Accidentally accessing offensive or pornographic material and failing to report the incident	√		√		√	√		√	
Deliberately accessing or trying to access offensive or pornographic material*	√		√		√	√	√	√	√
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	√		√		√	√	√	√	

*Consideration will be given as to whether a First Response referral needs to be made regarding social network or text abuse, pornographic images.

Staff	Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		√	√	√	√			√
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		√			√	√		
Unauthorised downloading or uploading of files		√			√	√		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		√			√	√		
Careless use of personal data eg holding or transferring data in an insecure manner		√				√		
Deliberate actions to breach data protection or network security rules		√	√		√			√
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		√			√			√
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		√	√					√
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		√	√					√
Actions which could compromise the staff member's professional standing		√				√		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		√	√					√
Using proxy sites or other means to subvert the school's filtering system		√	√	√	√			√
Accidentally accessing offensive or pornographic material and failing to report the incident		√	√		√	√		
Deliberately accessing or trying to access offensive or pornographic material		√	√	√	√		√	√
Breaching copyright or licensing regulations	√					√		
Continued infringements of the above, following previous warnings or sanctions		√	√	√	√		√	√

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when

infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority/Academy Group or national/local organisation (as relevant).
    - Police involvement and/or action

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

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- offences under the Computer Misuse Act (see User Actions chart above)
- other criminal conduct, activity or materials

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

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Cyber bullying
For the purpose of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images, online.

The school recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.

The school will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.

The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.

The school has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-bullying Policy.

The head teacher will decide whether it is appropriate to notify the police or see support from an external agency

On-line Safety and pupils with special educational needs
A pupil who has a learning difficulty or disability may be even more vulnerable to deceptive messages offering friendship or to opening dialogue on topics of mutual interest. These pupils are likely to need additional advice on safe behaviours and what they should never disclose to others online; they may also need increased supervision. This could include, for example, guidance that before entering dialogue with anyone new, they should always consult a trusted adult.

Review
This policy will be monitored and reviewed every 2 years unless there is a specific reason to review it earlier.

This policy should be read in conjunction with other school policies:
Safeguarding Policy/Child Protection Policy
Anti-Bullying/Cyber-Bullying Policy
Behaviour Policy
Equal Opportunities policy/Equality Policy
Staff behaviour Policy
SMSC Policy
PHSE Curriculum Statement

Appendix 1

Baldwins Gate CE Primary School
Acceptable use of the school's ICT facilities and internet: agreement for younger pupils and parents/carers

Name of pupil:

When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not:

- Use them without asking a teacher first or without a teacher in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson)
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes
- Share my password with others or log in using someone else's name or password
- Bully other people

☐ I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

☐ I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

☐ I will always be responsible when I use the school's ICT systems and internet.

☐ I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2

Baldwins Gate CE Primary School
Acceptable use of the internet: agreement for parents and carers

Name of parent/carer:

Name of child:

Online channels are an important way for parents/carers to communicate with, or about, our school.

The school uses the following channels:

- Our official Facebook page
- Email/text groups for parents (for school announcements and information)

Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way
- Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers

Signed:	**Date:**

Appendix 3

USE OF DIGITAL/VIDEO IMAGES

The use of digital/video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and school trips. These images may then be used in books, displays or presentations in subsequent lessons. We feel this is an important part of recording pupils learning and fun within school.

Images may also be used to celebrate success through their publication in newsletters, on the school website or social media and occasionally in the public media. Where an image is publicly shared by any means, only your child's first name will be used.

The school will comply with the Data Protection Act and request parent's/carer's permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should **not** be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children:

Name of child:	**Yes**	**No**
As the parent/carer of the above pupil, I agree to the school taking digital/video images of my child to support learning activities where they might be used in books, on displays, or in electronic presentations		
I agree for digital/ video images of my child to be used in the school newsletter, on the school website or school social media with only their first name used in publicity that reasonably celebrates success and promotes the work of the school.		
I agree to the school taking digital/video images of my child, such as assemblies, productions or class photographs that may be shared with other parents.		
I consent to images of my child being used on the school's Early Years and Key Stage 1 assessment system (currently Tapestry).		
I give permission for my child to be included in the school class photograph and I understand that this printed photo can be purchased by parents/carers		
I give permission for my child's photograph to be used in the media (eg the local press) on the understanding that I will be contacted beforehand to explain the context.		
I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by these guidelines in the use of these images.		
Please note: To respect everyone's privacy and in some cases protection, these images should **not** be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.		
Signed (Parent/Carer): **Date:**		

Consent can be withdrawn at any time. Please email office@baldwinsgate.staffs.sch.uk or speak to Mrs Riley in the school office if you wish to amend your consent.

Appendix 4

Online Safety Committee Terms of Reference

Online Safety Committee Members:

Mrs S Maude (Chair)
Mr J Ahearne
Mrs V Danks

1. Purpose
   To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives. The committee will also be responsible for regular reporting to the Full Governing Board

2. Membership

2.1 The online safety group will seek to include representation from all stakeholders.

The composition of the group should include:

- SLT member/s
- Child Protection/Safeguarding officer
- Teaching staff member
- Support staff member
- Online safety coordinator (not ICT coordinator by default)
- Governor
- Parent/Carer
- ICT Technical Support staff (where possible)

2.2 Other people may be invited to attend the meetings at the request of the Chair of this committee on behalf of the committee to provide advice and assistance where necessary.

2.3 Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4 Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature.

2.5 When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. Chair
   The Committee should select a suitable Chair from within the group. Their responsibilities include:
   - Scheduling meetings and notifying committee members;
   - Inviting other people to attend meetings when required by the committee;
   - Guiding the meeting according to the agenda and time available;
   - Ensuring all discussion items end with a decision, action or definite outcome;
   - Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. Duration of Meetings
   Meetings shall be held twice yearly. A special or extraordinary meeting may be called when and if deemed necessary.

5. Functions
   These are to assist the Online Safety Lead (or other relevant person) with the following:

   - To keep up to date with new developments in the area of online safety
   - To (at least) annually review and develop the online safety policy in line with new technologies and incidents
   - To monitor the delivery and impact of the online safety policy
   - To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching/learning/training.
   - To co-ordinate consultation with the whole school/academy community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through [add/delete as relevant]:
   - Staff meetings
   - Student/pupil forums (for advice and feedback)
   - Governors meetings
   - Surveys/questionnaires for students/pupils, parents/carers and staff
   - Parents evenings
   - Website/VLE/Newsletters
   - Online safety events
   - Internet Safety Day (annually held on the second Tuesday in February)
   - Other methodsAppend
   - To ensure that monitoring is carried out of Internet sites used across the school/academy
   - To monitor filtering/change control logs (e.g. requests for blocking/unblocking sites).
   - To monitor the safe use of data across the school/academy
   - To monitor incidents involving cyberbullying for staff and pupils

6. Amendments
   The terms of reference shall be reviewed annually from the date of approval.

   They may be altered to meet the current needs of all committee members, by agreement of the majority.

The above Terms of Reference have been agreed by the Full Governing Board.

Signed by (Chair of Committee):	
Date:	
Date for review:	