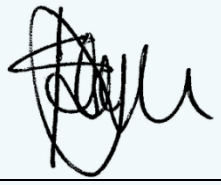
Digital Safeguarding Policy

2023-24*

***including acceptable use of ICT, social media, mobile phones and other wearable devices**



CEO SIGNATURE

CHAIR OF TRUST BOARD SIGNATURE

15/12/2023

DATE

Autumn 2024

NEXT REVIEW DATE

Contents

The Acceptable Use of the Internet, E-mail and Related Technologies

Why do we need a Digital Safeguarding Policy?

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including the senior leadership team), governors, volunteers and visitors.

However, the ICT resources and facilities our school uses could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents/carers and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

The provisions of the *Children Act 2004*, *Working Together to Safeguard Children* sets out how organisations and individuals should work together to safeguard and promote the welfare of children. The 'staying safe' outcome includes aims that children and young people are:

- *safe from maltreatment, neglect, violence and sexual exploitation*
- *safe from accidental injury and death*
- *safe from bullying and discrimination*
- *safe from crime and anti-social behaviour in and out of school*
- *secure, stable and cared for*.

Many of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

The Directors, Governors and SLT of St Bartholomew's CE Multi Academy Trust have a legal responsibility to safeguard children and staff and this includes online activity. E-Safety covers

issues relating to the safe use of the Internet, mobile phones and other electronic communications technologies (including wearable devices), both in and out of school. This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures. Breaches of this policy may be dealt with under our Staff Code of Conduct.

What are our Roles and Responsibilities?

Writing and reviewing the policy?

Our Digital Safeguarding Policy has been written by the Trust, building on exemplar policies from the SW Grid for Learning. The Digital Safeguarding Policy will operate in conjunction with other policies including those for Behaviour Management, Bullying, Curriculum, Safeguarding and Child Protection, Child on Child Abuse and Data Protection/GDPR. The Digital Safeguarding Policy will be agreed by the CEO and ratified by Directors. This policy is a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. Although many aspects will be informed by legislation and regulations, we will involve staff, governors, pupils and parents in writing and reviewing the policy and make sure the policy makes sense and it is possible to follow it in all respects. This will help ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice.

Staff

All staff should sign and follow the staff acceptable use policy (AUP) in conjunction with this policy, the school's main safeguarding policy, the code of conduct/handbook and relevant parts of Keeping Children Safe in Education to support a whole-school safeguarding approach.

This includes reporting any concerns, no matter how small, to the designated safety lead as named in the AUP, maintaining an awareness of current online safety issues and guidance (such as KCSIE), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond and avoiding scaring, victim-blaming language.

Staff should also be aware of the new DfE standards and relevant changes to filtering and monitoring and play their part in feeding back about over blocking, gaps in provision or pupils bypassing protections.

Headteacher

Key responsibilities:

- Foster a culture of safeguarding where online-safety is fully integrated into whole-school safeguarding
- Oversee and support the activities of the designated safeguarding lead team and ensure they work with technical colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school)
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance
- Ensure ALL staff undergo safeguarding training (including online-safety) at induction and with regular updates and that they agree and adhere to policies and procedures
- Ensure ALL governors and trustees undergo safeguarding and child protection training and updates (including online-safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles
- Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the new DfE standards—through regular liaison with technical colleagues and the DSL– in particular understand what is blocked or allowed for whom, when, and how as per KCSIE
    - In 2023/4 this will involve starting regular checks and annual reviews, upskilling the DSL and appointing a filtering and monitoring governor
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a compliant framework for storing data, but helping

to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets the needs of pupils, including risk of children being radicalised
- Ensure the school website meets statutory requirements

Designated Safeguarding Lead / Digital safeguarding Lead

Key responsibilities

- The DSL should "take **lead responsibility** for safeguarding and child protection (**including online safety and understanding the filtering and monitoring** systems and processes in place)
- Ensure "An effective whole school approach to online safety" as per KCSIE
- In 2023/4 working to take up the new responsibility for filtering and monitoring by working closely with technical colleagues, SLT and the new filtering governor to learn more about this area, better understand, review and drive the rationale behind systems in place and initiate regular checks and annual reviews, including support for devices in the home
- Where online-safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible but which cover areas of online safety (e.g. RSHE), ensure there is regular review and open communication and that the DSL's clear overarching responsibility for online safety is not compromised or messaging to pupils confused
- Ensure ALL staff and supply staff undergo safeguarding and child protection training (including online-safety) at induction and that this is regularly updated
    - In 2023/4 this must include filtering and monitoring and help them to understand their roles
    - All staff must read KCSIE Part 1 and all those working with children also Annex B
    - Cascade knowledge of risks and opportunities throughout the organisation.
- Ensure that ALL governors and trustees undergo safeguarding and child protection training (including online-safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated
- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns
- Be the primary contact for requests to unblock/block websites

- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online-safety and behaviour apply
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school)
- Work with the headteacher, DPO and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safeguarding and "undertake Prevent awareness training"
- Receive regular updates in online-safety issues and legislation, be aware of local and school trends
- Ensure that online-safety education is embedded across the curriculum in line with the statutory RSHE guidance
- Promote an awareness of and commitment to online-safety throughout the school community, with a strong focus on parents, including hard-to-reach parents
- Communicate regularly with SLT and the safeguarding governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when in isolation/quarantine
- Ensure staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying)

Each school's Safeguarding Lead ensures they keep up to date with E-Safety issues and guidance through liaison with our Computing advisors (E-Services) and through organisations such as The Child Exploitation and Online Protection (CEOP). The school's E-Safety Co-ordinator ensures the Headteacher (HT), Senior Leadership Team (SLT) and Governors/Directors are updated as necessary.

Governors

Key responsibilities

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board
- Undergo (and signpost all other governors and Trustees to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated
- Appoint a filtering and monitoring governor to work closely with the DSL on the new filtering and monitoring standards
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with the DPO, DSL and headteacher to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B
- Ensure that all staff undergo safeguarding and child protection training (including online safety and now also reminders about filtering and monitoring)
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum
- Consider a whole school approach to online safety with a clear policy on the use of mobile technology

Please see appendix A1 - Roles:

- PSHE / RSHE Lead/s
- Computing Lead
- Subject / aspect leaders
- Network Manager/technician
- Data Protection Officer (DPO)
- Volunteers and contractors (including tutor)
- Pupils
- Parents/carers
- External groups including parent associations

How will this policy be communicated?

This policy is a living document. It is accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the school website
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff and those starting mid-year)
- Integral to safeguarding updates and training for all staff
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups), which will be issued to whole school community, on entry to the school, annually and whenever changed and displayed in school

What are the main online safety risks in 2023/2024?

Current Online Safeguarding Trends

Self-generative artificial intelligence has been a significant change, with pupils having often unfettered access to tools that generate text and images at home or in school. These tools not only represent a challenge in terms of accuracy when young people are genuinely looking for information, but also in terms of safety. Schools not only need to tackle this in terms of what comes into school but also educating young people on use of these tools in the home.

Ofcom 'Children and parents: media use and attitudes report 2023' has shown that YouTube remains the most used site or app among all under 18s and the reach of WhatsApp, TikTok and Snapchat increased yet further. As a school we recognise that many of our children and young people are on these apps regardless of age limits. This is striking when you consider that 20% of 3-4 year olds have access to their OWN mobile phone, rising to over 90% by the end of Primary School, and the vast majority have no safety controls or limitations to prevent harm or access to inappropriate material. At the same time, even 3 to 6 year olds are being tricked into 'self-generated' sexual content (Internet Watch Foundation Annual Report) while considered to be safely using devices in the home and the 7-10 year old age group is the fastest growing for this form of child sexual abuse material, up 60% within 12 months to represent over 60,000 cases found.

Education and curriculum

It is important that our schools establish a carefully sequenced curriculum for online safety that builds on what pupils have already learned and identifies subject content that is appropriate for their stage of development.

As well as teaching about the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently regardless of the device, platform or app, Teaching Online Safety in Schools recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of pupils, including vulnerable pupils. RSHE guidance also recommends schools assess teaching to "identify where pupils need extra support or intervention (through) tests, written assignments or self-evaluations, to capture progress."

The following subjects have the clearest online safety links:

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)
- Computing
- Citizenship

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise.

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites. "Parents and carers are likely to find it helpful to understand what systems schools use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school (if anyone) their child is going to be interacting with online" (KCSIE 2023).

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. disinformation, misinformation and fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

At St Bartholomew's CE Multi Academy Trust, we recognise that online safety and broader digital resilience must be thread throughout the curriculum. Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to key areas of self-image and identity, online relationships, online reputation, online bullying, managing online information, health, wellbeing and lifestyle, privacy and security, and copyright and ownership.

Handling safeguarding concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship).

General concerns must be handled in the same way as any other safeguarding concern. Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online safety will be mostly detailed in the following policies:

- Safeguarding and Child Protection Policy
- Child-on-Child Abuse Policy
- Anti-Bullying Policy
- Behaviour Policy
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

This school commits to take all reasonable precautions to ensure safeguarding pupils online but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the digital safeguarding lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the headteacher unless the concern is about the headteacher in which case the complaint is referred to the

Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed (i.e. the local authority, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The DfE guidance Behaviour in Schools, advice for headteachers and school staff September 2022 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents – see pages 32-34 for guidance on child on child sexual violence and harassment, behaviour incidents online and mobile phones.

We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly concerning or breaks the law.

MANAGING INTERNET ACCESS

What about Copyright Laws?

The school will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law. Staff are not permitted to upload or display digital media without the permission of the owner, even if reproduced by pupils, as this can result in a fine or police action.

Material not covered by copyright law or original material is permitted to be uploaded or displayed. More concise and detailed information is available via gov.uk.

How will information systems security be maintained?

The security of the school information systems and users will be reviewed regularly. Virus protection will be updated regularly.

- *Personal data sent over the Internet or taken off site will be encrypted.*
- *Portable media may not used without specific permission followed by an anti-virus / malware scan.*
- *Unapproved software will not be allowed in work areas or attached to email.*
- *Files held on the school's network will be regularly checked.*
- *The ICT coordinator/network manager will review system capacity regularly.*
- *The use of user logins and passwords to access the school network will be enforced.*
- *The Department for Education's expected cyber security standards for schools will adhered to in respect of cyber security, user accounts and data protection (more detailed information is available via gov.uk here).*

How will email be managed?

Access in school to external personal e-mail accounts may be blocked by the school filtering system.

Pupils

- Pupils may only use approved whole school or group e-mail accounts on the school system.
- Through the teaching of the Computing and PSHE curriculum pupils will be informed that they must immediately tell a teacher or another trusted adult if they receive offensive e-mail, not reveal personal information or arrange to meet others without specific permission.

Staff

- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Group.
- E-mail sent to external organisations should be written carefully by the teacher and authorised by a member of SLT before sending, where appropriate, in the same way as a letter written on school headed paper.
- Staff should not use personal email accounts during school hours or for professional purposes.

How will published content and the school website be managed?

The contact details on each school website will be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published though staff names and photographs may be (subject to authorisation from the relevant members of staff). The headteacher will take overall editorial responsibility and will ensure that content published is accurate and appropriate. In the case of the MAT website, this is overseen by the CEO.

- Digital images/videos of children are stored in folders on the school's shared network.
- We do not use students' names when saving images in the file names.
- We do not include the full names of students in the credits of any video materials/DVDs produced and published by the school.
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of students.
- We gain written parental/carer permission for use of digital photographs or videos involving their child as part of the school agreement form when their daughter/son

joins the school. This may also be obtained on specific occasions where necessary e.g., trips, press opportunities etc.

- The NCSC's (National Cyber Security Centre) Web Check service is implemented across the Trust to review and monitor websites for common web vulnerabilities and misconfigurations.

How will social networking, social media and personal publishing be managed?

The school will control access to social media and social networking sites.

Pupils

- Through the Computing and PSHE curriculum the children will be taught about the appropriate use of these e.g., giving out personal information and the writing of unacceptable blogs. Pupils will be advised not to place personal photos on any social network space.
- Children will be taught how to protect themselves online and the four areas of risk: content, contact, conduct and commerce.

Staff

- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy. Staff are to be reminded that inappropriate use of these sites may result in disciplinary action being taken by the school. Attention will also be drawn to school Social Media Policy **(See Appendix E)**
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team.
- Staff must obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.

All members of the school community are advised not to publish specific and detailed private thoughts that may be considered threatening, hurtful, or defamatory.

Appropriate filtering and monitoring

Keeping Children Safe in Education has long asked schools to ensure "appropriate" web filtering and monitoring systems which keep children safe online but do not "overblock".

Since KCSIE 2023, in recognition of the importance of these systems to keeping children safe, the designated safeguarding lead now has lead responsibility for filtering and monitoring.

Schools are also asked to follow the new DfE filtering and monitoring standards, which require them to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs

Tech teams and safeguarding teams will need to work much more closely together for this to be possible and technicians will be charged to carry out regular checks and feed back to DSL teams.

ALL STAFF need to be aware of the changes and renewed emphasis and play their part in feeding back about areas of concern, potential for pupils to bypass systems and any potential overblocking. Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding, as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out. It is very important that schools understand the difference between filtering and monitoring, the meaning of overblocking and other terms, as well as how to get the best out of systems.

At St Bartholomew's CE Multi Academy Trust:

- web filtering is provided by Lightspeed, E2BN and RM SafetyNet on school site and for school devices used in the home (Lightspeed only), helping to ensure security standards are kept when students/teachers use devices away from school
- SENSO is used for monitoring across all of the schools, supported by Wolverhampton's E-Services, with the exception of Fairhaven, where Smoothwall is used
- reports are sent to the DSL and headteacher on violations. Headteacher's devices report to the CEO (any concerns or issues regarding monitoring or filtering can be addressed to E-Services)
- overall responsibility is held by the DSL

- technical support and advice, setup and configuration are from Wolverhampton E-Services/Concero.
- regular checks are made by the DSL to ensure filtering is still active and functioning everywhere (the recommended website for this is Check Your Internet Connection Blocks Child Abuse & Terrorist Content (swgfl.org.uk)
- an annual review is carried out as part of the online safety audit to ensure a whole school approach

According to the DfE standards, "a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

How will filtering be managed?

The school's SLT will ensure that regular checks are made to ensure that the filtering methods selected are effective.

Any material that the school believes is illegal will be reported to appropriate agencies such as CEOP.

The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

With regard to each school's filtering system, although every precaution is taken to ensure that inappropriate material is not accessed, the dynamic and ever changing nature of the internet means this material can never be fully stopped.

If an incident of inappropriate material being accessed occurs, staff are instructed to take a screen shot for filters to be amended.

How are emerging technologies managed?

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use Policy **(See Appendix D)**

How should personal data be protected?

Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 2018/GDPR in line with the Data Protection Policy.

DECISIONS INFORMING THIS POLICY

How will Internet access be authorised?

Pupils and staff have access to the internet throughout their time at school. The school Internet access includes filtering appropriate to the age of pupils, which is provided by Wolverhampton E-Services and Concero.

Pupils' access to the Internet will always be supervised by an adult with access to specific and approved online materials. Children will use age-appropriate search engines (www.Kiddle.co.uk) and online tools and online activities will be teacher-directed where necessary.

The school office will maintain a current electronic record of all staff and pupils who are granted access to the school's electronic communications. This is stored on the Learning Platform.

Each user with access to the digital media is issued with a unique username and password in order to access class websites and emails.

For class based activities the pupils' laptops will either use a generic class password or the children will login to the laptops using their own logins, staff all have access to these passwords and staff manage their profiles. Arrangements will be school-specific.

How will risks be assessed?

The school will take all reasonable precautions to ensure that users access only appropriate material.

The school will audit ICT use to establish if the Digital Safeguarding policy is adequate and that the implementation of the Digital safeguarding policy is appropriate. Methods to identify, assess and minimise risks will be reviewed regularly.

How will the school respond to any incidents of concern?

In the first instance, the Digital Safeguarding Lead will be informed, unless there are immediate safeguarding concerns, who will record the incidents and actions taken on the recording system used in school.

The Designated Safeguarding Lead(s) will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately (**See Appendix G**).

The school will inform parents/carers of any incidents or concerns as and when required. Where there is cause for concern or fear that illegal activity has taken or is taking place then the school will contact the Children's Safeguarding Team or Digital Safeguarding Lead and escalate the concern to the Police. After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required. (**See Appendix G)**

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher (refer to our behaviour policy) can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils
- Is identified in the school rules as a banned item for which a search can be carried out
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher (or DSL or appropriate staff member)
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine **(unless the staff member suspects a device may contain an indecent image of a child)**, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so. When deciding whether there is a 'good reason' to examine data or files on

an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm
- Undermine the safe environment of the school or disrupt teaching
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member and headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL or deputy immediately, who will decide what to do next

The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for educational settings working with children and young people. Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

How will digital safeguarding complaints be handled?

Complaints about the misuse of the Internet or any other ICT equipment will be dealt with by our Digital Safeguarding Lead in the first instance. Complaints about Internet misuse will be dealt with under the Trust's Complaints procedure. All Digital Safeguarding complaints and incidents will be recorded by the school, including any actions taken recorded on the school's recording system.

- *Any complaint about staff misuse will be referred to the HT or CEO if the complaint relates to use by a HT or member of the Trust's central support team*
- *Complaints of cyberbullying will be dealt with in accordance with our Anti-Bullying Policy and Child on Child Abuse Policy*
- *Complaints related to child protection are dealt with in accordance with Trust's Safeguarding and Child Protection procedures*

Any issues (including sanctions) will be dealt with according to the Trust's disciplinary, behaviour and child protection procedures. (**See Appendix G**)

Parents and pupils will need to work in partnership with staff to resolve issues.

How will Learning Platforms be managed?

The SLT will regularly monitor the use of the Learning Platform by pupils and staff in all areas, in particular message and communication tools and publishing facilities.

Only members of the current pupil and staff community will have access to the Learning Platform.

All users will be mindful of copyright issues and will only upload appropriate content onto the Learning Platform.

When staff, pupils etc. leave the school, their account or rights to specific school areas will be disabled or transferred to their new establishment.

All uploaded content is automatically tagged, and recorded by ICT Support, logging when and by whom it was uploaded.

How will mobile phones and personal devices (including wearable devices) be managed?

Mobile phones and other personal devices are considered to be an everyday item in today's society and many of our children may own and use personal devices to get online regularly.

Children's Use

- Mobile phones and wearable devices are permitted to be held in school during the school day
- Mobile phones and wearable devices are to be kept in a secure location, at the owner's risk. Children are not permitted to use their mobile phone or wearable device during the school day under any circumstances. If any pupil needs to contact parents/carers from school, this will be offered via a school landline

Staff Use

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity without express permission from the HT
- Mobile phones and wearable devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or wearable devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances
- Staff should not use personal devices to take photos or videos of pupils and will only use work-provided equipment for this purpose

All members of the St Bart's CE MAT community

- All members of St Bart's CE MAT community are advised to take steps to protect their mobile phones or personal devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises
- All members of St Bart's CE MAT community are advised to lock their devices securely to ensure that unauthorised calls or actions cannot be made on their phones or devices; this should be kept confidential and mobile phones and personal devices should not be shared
- Mobile phones and personal devices are not permitted to be used in any areas where there are children
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will

be dealt with in line with our anti-bullying and behaviour policies as well as the staff code of conduct and disciplinary procedures

- All members of St Bart's CE MAT community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies. If a member of staff breaches the school policy, then disciplinary action may be taken.

If visitors are required to take photographs/videos which include pupils as part of their professional work, this must be via a work device (not a personal device) with prior authorisation from the School (the School in turn will have signed agreements from parents with regard to use of their child(ren)'s image(s)). Where visitors need to take photographs/videos around school for work purposes, and these do not need to include images of pupils, the visitor will be escorted throughout their visit by a member of staff who will check the photographs/videos taken. Visitors are not permitted to use their personal devices to record any images or videos of any children whilst working in the school and will be reminded to turn their phones off and requested to delete any images if found to have taken any. In extreme cases they may also be asked to leave the site.

NB parents/carers are permitted to take photos/videos of their own children e.g. whilst attending a school performance but are requested not to upload these to social media sites if they include any other children.

Please also refer to Overview of Sexting Guidance.pdf (publishing.service.gov.uk) and Searching, screening and confiscation in schools - GOV.UK (www.gov.uk).

PHYSICAL AND TECHNICAL SECURITY

Each piece of ICT equipment is logged with a serial number, matching inventory code and owner. This is kept by the E-service provider and school office.

Each member of staff who has been assigned digital equipment will have signed a laptop and digital camera agreement outlining the acceptable use of the equipment **(See Appendix C)**. A copy is kept in the staff member's personnel file.

The school's system is constantly updated and scanned by the local authority on a regular basis. The system has an up to date firewall, filtering and antivirus software.

Staff who manage filtering systems or monitor ICT use will be supervised by the SLT and have clear procedures for reporting issues.

Any breaches are reported to the E-service provider automatically but should also be relayed to the e-safety lead teacher immediately.

TRAINING, EDUCATION & POLICY COMMUNICATION

This policy is available on the school website and will be referenced in newsletters and the school prospectus.

Up-to-date and appropriate staff training in safe and responsible internet use, both professionally and personally, will be provided for all members of staff. It is the responsibility of the e-safety lead teacher to ensure that all stakeholders are provided with the appropriate training and support according to their needs.

All visitors to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy **(See Appendix A)**

Pupils

- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas and will precede internet access
- An e–safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for Internet use
- Age appropriate Digital Safeguarding rules or copies of the Pupil Acceptable Use Policy will be posted in all rooms with Internet access **(See Appendix B)**
- Pupils will also be asked to read and sign the School Acceptable Use Agreement for pupil access **(See Appendices B1 and B2)** and discuss it with their parent as part of the Home school Agreement **(See Appendix F)**

Staff

Staff are to be made aware that all internet use in school is logged automatically and can be traced to the individual user.

- The Digital Safeguarding Policy will be formally provided to and discussed with all members of staff annually and will from part of the induction procedures for new members of staff

- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All staff will read and sign the School Acceptable Use Agreement before using any school ICT resources **(See Appendix D)**

Parents

Parents' attention will be drawn to the school Digital Safeguarding Policy in newsletters, the school prospectus and on the school website.

- A partnership approach to e-safety at home and at school with parents will be encouraged.
- Parents will be requested to sign digital safeguarding/ICT agreement as part of the Home School Agreement and discuss its implications with their children as part of the Home School Agreement **(See Appendix F).**
- Information and guidance for parents on digital safeguarding will be made available to parents.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.

Appendix A1: Roles

PSHE / RSHE Lead/s

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from recent trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives."
- Focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools in an age appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to "identify where pupils need extra support or intervention [through] tests, written assignments or self-evaluations, to capture progress".
- Work closely with the DSL/Digital SL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach.

Computing Lead

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum.
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach.
- Work closely with the DSL/Digital SL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements.

Subject Leaders
Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the RSHE curriculum, and model positive attitudes and approaches to staff and pupils alike.
- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context.
- Work closely with the DSL/Digital SL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Ensure subject specific action plans also have an online-safety element.

Network Manager/other technical support roles – (Chris Watabiki)
Key responsibilities:

- As listed in the 'all staff' section, plus:
- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.
- Note that KCSIE changes expect a great understanding of technology and its role in safeguarding when it comes to filtering and monitoring and in 2023/4 you will be required to support safeguarding teams to understand and manage these systems and carry out regular reviews and annual checks.
- Support DSLs and SLT to carry out an annual online safety audit as now recommended in KCSIE. This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'overblocking' is avoided as per KCSIE) to support their role as per the new DfE standards, protections for pupils in the home and remote-learning.
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Work closely with the designated safeguarding lead / digital safeguarding lead / data protection officer / RSHE lead to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice.
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms, etc.

- Maintain up-to-date documentation of the school's online security and technical procedures.
- To report online-safety related issues that come to their attention in line with school policy.
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Ensure the data protection policy and cybersecurity policy are up to date, easy to follow and practicable.
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy
- Work with the Headteacher to ensure the school website meets statutory DfE requirements.

Data Protection Officer (DPO) – (Chris Dryer)
Key responsibilities:

- Alongside those of other staff, provide data protection expertise and training and support the DP and cybersecurity policy and compliance with those and legislation and ensure that the policies conform with each other and with this policy.
- Not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools*, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2023, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."
- Note that retention schedules for safeguarding records.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.

Volunteers and contractors (including tutor)
Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP).
- Report any concerns, no matter how small, to the designated safety lead.
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications.

Pupils
Key responsibilities:

- Read, understand, sign and adhere to the pupil acceptable use policy.

Parents/carers
Key responsibilities:

- Read, sign and adhere to the school's parental acceptable use policy (AUP), read the pupil AUP and encourage their children to follow it.

External groups including parent associations
Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school.
- Support the school in promoting online safety and data protection.
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

Appendix A: Visitor Acceptable Use Agreement / Code of conduct

ICT and the related technologies such as email, the internet, mobile phones and wearable devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All visitors who require access to the internet are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the School e-safety Lead.

When using school equipment please follow these guides to ensure our children remain safe digitally -

- **I will NOT attempt to install programs of any type on the computers.**
- **I will always check files brought in on removable media (such as CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses.**
- I will protect the computers from spillages by eating or drinking well away from the ICT equipment.
- All visitors must follow the guidelines even when using their own equipment – I will read and be familiar with the Trust's Digital Safeguarding Policy and will follow the procedures detailed within it.
- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the HT/HOS and/or Governors/Directors.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not browse, download or upload material that could be considered offensive or illegal.
- I will not send to pupils or colleagues material that could be considered offensive or illegal.
- Images of pupils will only be taken using school equipment and used for professional purposes and will not be distributed outside the school network without the permission of the parent/ carer and the HT/HOS.
- I will not use mobile devices whilst at school unless I have permission from the HT/HOS/CEO.
- I will use wearable devices – such as fitness trackers or smart watches – in a responsible manner and not in front of children.

- I will not use mobile or wearable devices to photograph or video children/staff
- I will respect copyright and intellectual property rights.
- I will support and promote the Trust's Digital Safeguarding policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will report any misuse or inadvertent exposure to inappropriate conduct.
- I understand that any infringement of these rules may be treated as misconduct or gross misconduct.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school(s).

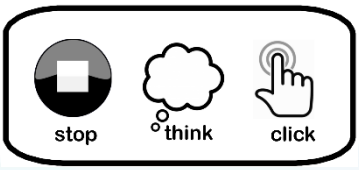
Signature …….. Date ……

Full Name …….. (printed)

Job title…….

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If you violate these provisions, access to the Internet will be denied and you will be subject to disciplinary action. Additional action may be taken by the school in line with existing policy regarding staff behaviour. Where appropriate, police may be involved or other legal action taken

Appendix B1: Acceptable Use Policy Agreement KS2



Keeping safe: stop, think, before you click!

Our school uses computers and other pieces of technology e.g. *iPads, Kindles, cameras* etc and provides us with Internet access to help our learning.

These rules will keep everyone safe and help us to be fair to others:

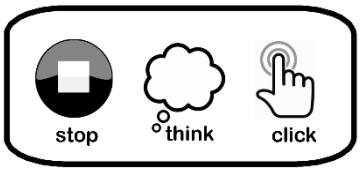
- I will ask permission from a member of staff before using the Internet
- I will use only my own logins and password, which I will keep secret
- I will only access my own files, and I will not access or change other people's files or information
- I will only change the settings on the computer if a teacher has allowed me to
- I only use websites and search engines that my teacher has chosen
- I understand that the school/setting internet filter is there to protect me, and I will not try to bypass it
- I will use all devices only for school work and home learning
- I will not bring in memory sticks unless I have been given permission
- I will only use e-mail or post on the year group sites – including photos/videos - if my teacher has given me permission
- I only open messages and talk with people I know, and I only click on links if I know they are safe
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult
- I know that not everything or everyone online is honest or truthful
- I will check content on other sources like other websites, books or with a trusted adult

- I always credit the person or source that created any work, image or text I use
- The messages I send will be polite, friendly and responsible
- I will not share my home address, phone number or any other personal information with anyone else when I am on the internet
- To help protect everyone, I will tell a teacher or another trusted adult if I see anything I am unhappy with or if I receive messages I do not like, including any potentially unsafe behaviour or actions of other children in school
- I understand that the school may check my computer files and may monitor the Internet sites I visit
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online

Pupil Signature : ……..

Class:……. Date: ……..

'Correct Internet and Email use in the Classroom' to be signed by parent/guardian when child joins each school.



Appendix B2: Acceptable Use Policy Agreement KS1 and Foundation

Keeping safe: stop, think, before you click! How to stay safe online

This is how we stay safe in school when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I only use the internet when an adult is with me
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I only click on links and buttons online when I know what they do
- I keep my personal information and passwords safe
- I only send messages online which are polite and friendly
- I know the school I can visit www.thinkuknow.co.uk to learn more about keeping safe online
- I know that adults in school can see what I am doing online
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules, I might not be allowed to use a computer / tablet

Signed (child): …….

Class: …….

Date …….

'Correct Internet and Email use in the Classroom' to be signed by parent/guardian when child joins each school

Appendix C: School Laptop, Digital Camera and Tablet Agreement

This document is an agreement between both staff and school/Trust, and shall be binding for the duration employment at the school/Trust.

General conditions

1. The laptop, Digital Camera and tablet shall remain the property of the school/Trust.
2. The laptop, Digital Camera and tablet shall be retained by staff in order to exercise their professional duties.
3. The laptop, Digital Camera and tablet shall be returned to school upon a member of staff leaving school to take up a post elsewhere and any additional software/saved data removed.
4. Staff are to take good care of the laptop, Digital Camera and tablet at all times.
5. Staff shall be responsible for the security of the laptop, Digital Camera and tablet, ensuring it is in a lockable cupboard when unattended in school and ensuring all reasonable precautions are taken when transporting the laptop, Digital Camera and tablet.
6. Any additional software installed on the laptop, Digital Camera and tablet is to be correctly licensed.
7. All faults are to be reported and logged by the user on the School Learning Platform for the ICT Support Service Team and will be ultimately prioritised by the Computing Co-ordinator in School

Use conditions

1. The laptop, Digital Camera and tablet MUST be available for use in school each day. In the case of long term absences, all reasonable attempts should be made to return equipment to school.
2. Staff shall be aware of the issues relating to access to Internet sites not relevant or appropriate to their professional duties.
3. Staff shall operate Internet access with due regard to school and Wolverhampton City Council policies.
4. Staff shall use the laptop, Digital Camera and tablet in a responsible and professional manner.
5. Staff will be expected to use the laptop, Digital Camera and tablet for:
   - Planning
   - Delivery of lesson
   - Record Keeping

- Analysis of assessment
- Target Setting
- Accessing Learning Platform
- Communicating with parents

Any other professional duties
The school agrees to provide training for teachers in order to make effective use of their laptop, Digital Camera and tablet.

Any personal data held on the laptop, Digital Camera and tablet such as music, pictures or other personal files are the responsibility of the individual and the school / ICT Support Service cannot be held responsible for loss, theft or damage of these. We advise that any personal files of any nature are backed up in addition to the normal laptop, Digital Camera and tablet synchronisation.

I agree to the terms and conditions stated above.

Print Name…… Signed …….
Date……..
Signed on behalf of school …… Date:……..
Laptop Serial / Service Tag Number .....
Asset Number……..
Digital Camera Serial / Service Tag Number .....
Asset Number……..
Tablet serial/service tag number .....
Asset Number……..

Appendix D: Acceptable Use Agreement – Staff Acceptable Use Agreement / Code of conduct

ICT and the related technologies such as email, the internet, mobile phones and wearable devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the School e-Safety coordinator.

The computers are provided and maintained for the benefit of all staff, and you are encouraged to use and enjoy these resources, and help to ensure they remain available to all. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

This policy should be read in conjunction with the staff Code of Conduct policy.

- I will get permission before installing, attempting to install or storing programs of any type on the computers.
- I will check files brought in on removable media (such as CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses.
- I will check mobile equipment (e.g. laptops, tablet PCs, PDAs etc.) with antivirus software and ensure they have been found to be clean of viruses before connecting them to the network.
- I will protect the computers from spillages by eating or drinking well away from the ICT equipment.
- I will read and be familiar with the school digital safeguarding policy and will follow the procedures detailed within it.
- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the HT/HOS and/or Governors/Directors.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.
- I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to our ICT support provider.
- I will not keep documents which contain school-related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as

laptops, digital cameras, and mobile phones. Where possible, I will use SharePoint to upload any work documents and files in a password protected environment.

- I will not browse, download or upload material that could be considered offensive or illegal.
- I will not send to pupils or colleagues material that could be considered offensive or illegal.
- Images of pupils will only be taken using school equipment and used for professional purposes and will not be distributed outside the school network without the permission of the parent/ carer.
- I will not use mobile devices whilst at school unless I have permission from the Head Teacher.
- I will use wearable devices – such as fitness trackers or smart watches – in a responsible manner and not in front of children.
- I will not use mobile or wearable devices to photograph or video children/staff.
- I will not attempt to bypass any filtering and/or security systems put in place by the school.
- I will respect copyright and intellectual property rights.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will report any misuse or inadvertent exposure to inappropriate conduct.
- I understand that any infringement of these rules may be treated as misconduct or gross misconduct.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature …….. Date ……

Full Name …….. (printed)

Job title…….

Appendix E: Social Media Policy

Legislation

Human Rights Act 1998 - being mindful of employees' activities outside work – the policy does not intend to limit sensible, personal, non-work related private use of social media.

Public Interest Disclosure Act 1998 – how employees should handle this - if you believe there is wrong doing in your workplace (e.g. your employer is committing a criminal offence) you can report this by following the correct processes, and your employment rights are protected.

Case Law involving employee relations disputes – Head teachers should seek advice from Schools HR Team - Human Resources Consultant.

Equalities Act 2010, Data Protection Act 2018 and the CCTV Code of Practice 2008 (Information Commissioners Office), Computer Misuse Act 1990, Copyright, Design & Patents Act 1988,

Regulation of Investigatory Powers Act 2000

Staff personal use of social media

- The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional online behaviour is outlined for all members of staff, including volunteers, as part of our code of conduct and acceptable use of technology policy.
- Any complaint about staff misuse or policy breaches will be referred to the HT/HOS, in accordance with our allegations against staff policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- If appropriate, disciplinary, civil and/or legal action will be taken in accordance with our staff code of conduct.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the School/Trust.

- Civil, legal or disciplinary action may be taken if staff are found to bring the profession or school/Trust into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media services. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include, but is not limited to:
    - Setting appropriate privacy levels on their personal accounts/sites.
    - Being aware of the implications of using location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Using strong passwords.
- Ensuring staff do not represent their personal views as being that of the School/Trust.
- Members of staff are encouraged not to identify themselves as employees of the School/trust on their personal social networking accounts; this is to prevent information being linked with the setting and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online. Staff are expected to ensure that their social media use is compatible with their professional role and is in accordance with our policies, and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues, will not be shared or discussed on social media sites.
- Members of staff will notify the leadership team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents/carers

- Staff will not use any personal social media accounts to contact pupils or parents/carers, nor should any contact be accepted.

- All members of staff are advised not to communicate with or add any current or past pupils or their family members, as 'friends' on any personal social media sites, applications or profiles.
- Any pre-existing relationships or exceptions which compromise this requirement will be discussed with the DSL and/or the HT/HOS.
- Decisions made and advice provided in these situations will be formally recorded in order to safeguard pupils, the setting and members of staff.
- If ongoing contact with pupils is required once they have left the setting, members of staff will be expected to use existing alumni networks, or use official setting-provided communication tools.
- Any communication from pupils and parents received on personal social media accounts will be reported to the DSL (or deputy) and/or the HT/HOS.

Pupils' use of social media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach via age-appropriate sites and resources.
- We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we will not create accounts for pupils under the required age as outlined in the services terms and conditions.
- Pupils will be advised:
    - to consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location.
    - to only approve and invite known friends on social media sites and to deny access to others by making profiles private.
    - not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so when a trusted adult is present.
    - to use safe passwords.
    - to use social media sites which are appropriate for their age and abilities.
    - how to block and report unwanted communications.

    - how to report concerns on social media, both within the setting and externally.

- Any concerns regarding pupils' use of social media will be dealt with in accordance with existing policies, including anti-bullying, safeguarding and child protection and behaviour.
- The DSL (or deputy) will respond to online safety concerns involving safeguarding or child protection risks in line with our safeguarding and child protection policy.
- Sanctions and/or pastoral/welfare support will be implemented and offered to pupils as appropriate, in line with our behaviour policy. Civil or legal action will be taken if necessary.
- Concerns regarding pupils' use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.

Official use of social media

- St Bart's CE MAT's official social media channels are: Twitter for each school. In addition, our schools utilise Class Dojo for home learning and communication between pupils and staff, which is classed as social media as per the Class Dojo Privacy Policy.
- The official use of social media sites by St Bart's CE MAT's schools only takes place with clear educational or community engagement objectives and with specific intended outcomes.
- The official use of social media as a communication tool has been formally risk assessed and approved by the HT/HOS.
- Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.
- Staff use setting-provided email addresses to register for and manage official social media channels.
- Official social media sites are suitably protected and, where possible, run and/or linked to/from our website.

- Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including but not limited to anti-bullying, image/camera use, data protection, confidentiality and safeguarding and child protection.
- All communication on official social media platforms by staff on behalf of the School/Trust will be clear, transparent and open to scrutiny.
- Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
- Any official social media activity involving pupils will be moderated if possible.
- Parents and carers will be informed of any official social media use with pupils; written parental consent will be obtained, as required.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.
- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professional accounts where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the School/Trust, they will:
    - Sign our acceptable use policy.
    - Be aware they are an ambassador for the School/Trust.
    - Be professional, responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection and equalities laws.
    - Ensure appropriate consent has been given before sharing images on the official social media channel.

- Not disclose information, make commitments or engage in activities on behalf of the School/Trust, unless they are authorised to do so.
- Not engage with any private/direct messaging with current or past pupils or parents/carers.
- Inform their line manager, the DSL (or deputy) and/or the HT/HOS of any concerns, such as criticism, inappropriate content or contact from pupils.

Appendix F: HOME SCHOOL AGREEMENT

This document is signed by all parents when their child joins the School.

Child's Name: ……

The Parents/Carers

I/We will try to:

- Ensure my child attends school regularly, on time and properly equipped.
- Inform the school about concerns or issues that may affect my child's learning.
- Support the core values of the School.
- Support my child with home learning and specific homework tasks.
- Attend parent meetings and discussions about my child's progress.
- Be involved with my child's life at school.
- Not create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate.

The Child

I will try to:

- Attend school regularly and on time.
- Be well organised and have the equipment I need each day.
- Follow the School's core values.
- Work hard at school and complete homework so that I make good progress.

The School

We will:

- Provide a caring and safe learning environment.
- Promote the School's core values and achieve high standards.
- Support and challenge your child to make good progress and achieve their potential.
- Offer a relevant curriculum for learning that motivates your child to develop key learning skills.
- Promote healthy lifestyles.
- Develop positive working relationships and open communication.
- Keep parents/carers informed about their child's progress and concerns.

Signed: …… (HT/HOS) Date: ……

Signed: …… (child) Date: ……

Signed: …… (Parent/Carer) Date: ……

Correct Internet and Email use in the Classroom

I will not do any of the following:

- I will not change other people's work without their permission.
- I will only use the computers for school work and homework.
- I will not change desktop settings or alter the school's computers in any way.

If I break any of these rules, I understand that I may not be able to use the school's computing equipment.

Students will not be allowed to take part in an Internet lesson until the school receives the completed form.

Child Commitment

I agree to use the internet correctly and in a responsible way.

Name (block capitals): ……..

Signature: …… Date: ……..

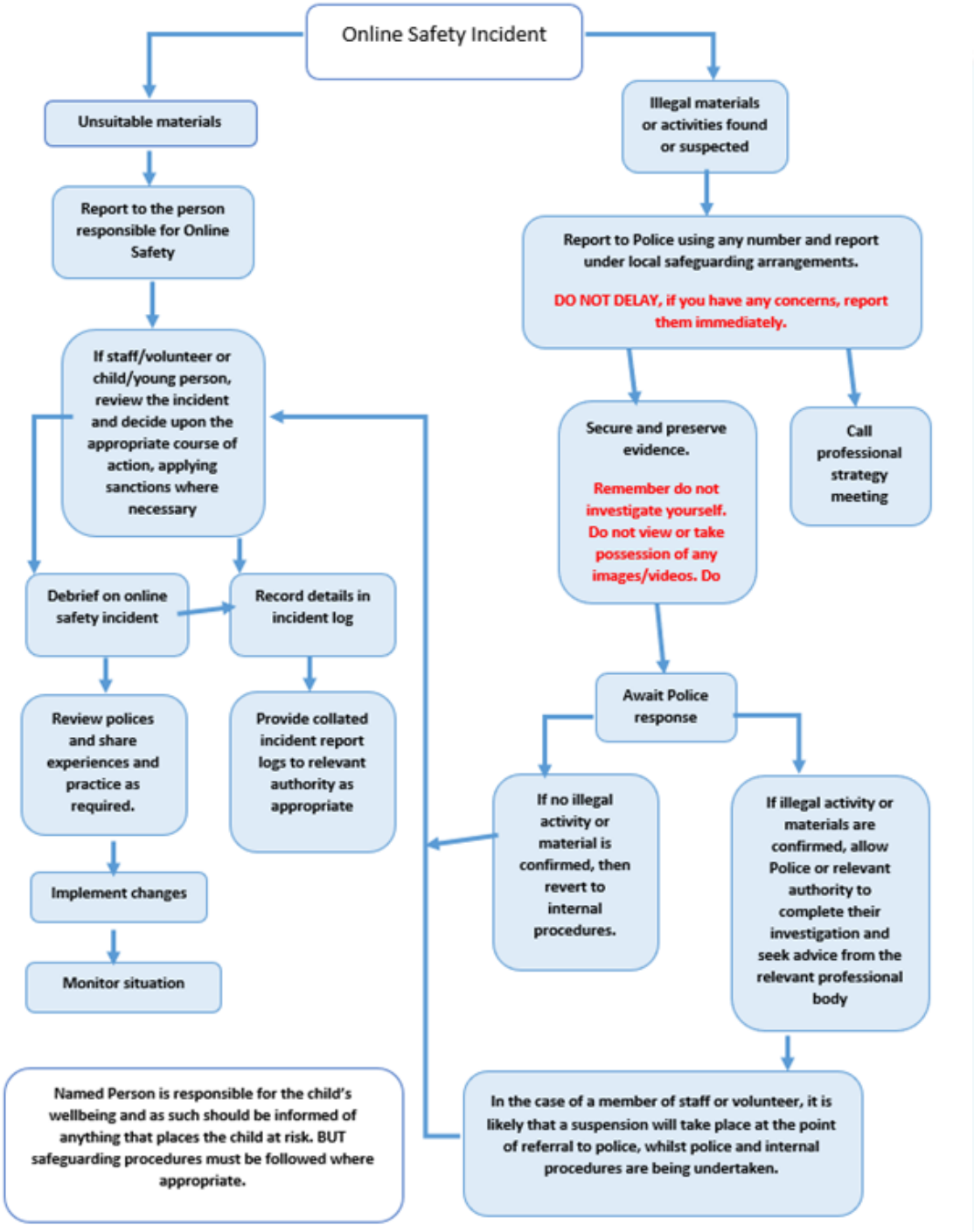
Parent Statement

As the parent (or legal guardian) of the above child I give him/her permission to use the Internet and I have read and understood the above rules. I have discussed the implications of breaking them with my son/daughter. I understand that I may withdraw my consent for my child to use the Internet at any time, which I will do in writing to the main school office.

Name (block capitals): ……..

Signature: …… Date: ……..

Appendix G1: Flowchart for responding to online safety incidents



Appendix G2: Young people

Incidents:	Refer to HT/HOS	Refer to Police	Requires technical responses/support	Inform parents and carers	Removal of access to technology /devices*	Warning	Further sanction – exclusion*
Accessing or trying to access illegal material (see list in earlier section on unsuitable / inappropriate activities).	✓		✓	✓	✓		
Unauthorised downloading or uploading	✓		✓		✓		
Allowing others to access technology / devices by sharing username and passwords	✓		✓		✓		
Attempting to access or accessing the technology / devices, using another person's account (hacking)	✓		✓	✓	✓		
Corrupting or destroying the data of other users	✓		✓	✓	✓		
Sending a communication that is regarded as offensive, harassment or of a bullying nature	✓			✓	✓		✓
Actions which could bring the organisation into disrepute.	✓			✓	✓		
Deliberately accessing materials that the school has agreed is inappropriate	✓		✓	✓	✓		
Activities that infringe copyright or data protection.	✓		✓			✓	
Using proxy by-pass sites or other means to subvert the filtering system	✓		✓	✓	✓		
Accidentally accessing materials that the school has agreed is inappropriate and failing to report it.	✓		✓			✓	
Unauthorised use of mobile phone / digital camera / other handheld/wearable device	✓		✓	✓		✓	
Unauthorised use of social networking / instant messaging / personal email	✓		✓	✓		✓	

*Amount of time dependent upon the severity of the incident

Appendix G3: Staff and volunteers

Incidents:	Refer to line manager / HT/HOS	Refer to National / Local Organisation / body	Refer to Police * *always refer if action deemed illegal*	Requires technical response / support	Warning	Suspension	Disciplinary action
Accessing or trying to access illegal material (see list in earlier section on unsuitable / inappropriate activities).	✓						
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email "while at work"	✓						
Unauthorised downloading or uploading of files	✓						
Disclosing passwords or any information relating to the security of technology and devices.	✓						
Accidental infringement of the organisation's personal data policy	✓						
Deliberate infringement of the organisation's personal data policy	✓						
Corrupting or destroying the data of other users	✓						
Deliberate damage to hardware or software	✓						
Sending a communication that is offensive, harassment or of a bullying nature	✓						
Using personal communication technologies e.g. email / social networking / instant messaging / text messaging to communicate with young people (except where allowed in the policy)	✓						
Actions which could compromise the professional integrity of staff / volunteers	✓						
Bringing the organisation into disrepute	✓						
Deliberately accessing materials that the group has agreed is inappropriate	✓						
Breaching copyright or licensing regulations	✓						
Using proxy by-pass sites or other means to subvert the filtering system	✓						
Accidentally accessing materials that the group has agreed is inappropriate and failing to report it.	✓						

Appendix H: Social Media Policy

Introduction
Employees of St Bart's CE MAT may be able to access social media services and social networking websites at work, either through company IT systems or via their own personal equipment.

This social media policy describes the rules governing use of social media at St Bart's CE MAT's Schools. It sets out how staff behave when using the company's social media accounts. It also explains the rules about using personal social media accounts at work and describes what staff may say about the company on their personal accounts.

This policy should be read alongside other key policies.

Why this policy exists
Social media can bring significant benefits to schools, particularly for building relationships with parents and the wider community. However, it's important that staff who use social media within the school do so in a way that enhances the school. A misjudged status update can generate complaints or damage to the school's reputation. There are also security and data protection issues to consider.

This policy explains how employees can use the social media safely and effectively.

Policy scope
This policy applies to all staff. Contractors and volunteers at our schools who use social media while working – no matter whether for business or personal reasons.

It applies no matter whether that social media use takes place on school premises, while travelling during work time or while working from home.

Social media sites and services include (but are not limited to):

- Popular social networks like **Twitter** and **Facebook**
- Online review websites like **Revoo**
- Sharing and discussion sites like **Reddit**
- Photographic social networks like **Instagram** and **Snapchat**
- Question and answer social network sites like **Quora** and **Yahoo answers**
- Professional social network sites like **LinkedIn**

Responsibilities

Everyone who operates a school social media account or who uses their personal social media accounts at school has some responsibility for implementing this policy.

However, these people have key responsibilities:

- The CEO is ultimately responsible for ensuring that St Bart's CE MAT's Schools use social media safely, appropriately and in line with the Trust's objectives. Monitoring and implementation of this is delegated to the HT/HOS for each school.
- The E-Services is responsible for providing apps and tools to manage the school's social media presence and track and key performance indicators. They are also responsible for proactively monitoring for social media security threats.
- The Assistant HT/HOS is responsible for working with the HT/HOS to roll out marketing ideas and campaigns through our social media channels.
- The senior leadership team (SLT) is responsible for ensuring requests for assistance and support made via social media are followed up.

General social media guidelines

The power of social media

St Bart's CE MAT recognises that social media offers a platform for schools to perform marketing, stay connected with parents and pupils and build profiles online.

The Trust also believes its staff should be involved in professional conversations on social networks. Social media is an excellent way for staff to make useful connections, share idea and shape discussions.

The Trust therefore encourages staff to use social media to support the school's goals and objectives.

Basic advice

Regardless of which social networks staff are using, or whether they're using school or personal accounts during school time, following these simple rules helps avoid the most common pitfalls:

- **Know the social network.** Staff should spend time becoming familiar with the social network before contributing. It's important to read any FAQs and understand what is and is not acceptable on a network before posting messages or updates.
- **If unsure, don't post it.** Staff should err on the side of caution when posting to social networks. If an employee feels an update or message might cause complaints or

offence– or be otherwise unsuitable – they should not post it. Staff members can always consult the HT/HOS for advice.

- **Be thoughtful and polite.** Many social media users have got into trouble simply be failing to observe basic good manners online. Staff should adopt the same level of courtesy used when communicating via email.
- **Look out for security threats.** Staff members should be on guard for social engineering and phishing attempts. Social networks are also used to distribute spam and malware. Further details below.
- **Keep personal use reasonable.** Although the school believes that having staff who are active on social media can be valuable both to the staff and to the school, staff should exercise restraint in how much personal use of social media they make during working hours.
- **Don't make promises without checking.** Some social networks are very public, so staff should not make any commitments or promises on behalf of the Trust's Schools without checking that the school can deliver on the promises. Direct any enquiries to the HT/HOS.
- **Handle complex queries via other channels.** Social networks are not a good place to resolve complicated enquiries and issues. Once a parent or member of the wider community has made contact, staff should handle further communications via the most appropriate channel – usually email or telephone.
- **Don't escalate things.** It's easy to post a quick response to contentious status update and then regret it. Employees should always take the time to think before responding, and hold back it they are in any doubt at all.

Use of school social media accounts

This part of the social media policy covers all use of social media accounts owned and run by the school.

Authorised users

Only people who have been authorised to use the school's social networking accounts may do so.

Authorisation is usually provided by the HT/HOS. It is typically granted when social media-related tasks form a core part of a staff's job.

Allowing only designated people to use the accounts ensures the school's social media presence is consistent and cohesive.

Creating social media accounts

New social media accounts in the school's name must not be created unless approved by the HT/HOS.

Each school operates its social media presence in line with a strategy that focuses on the most appropriate social networks, given available resources.

If there is a case to be made for opening a new account, employees should raise this with the HT/HOS.

Purpose of school social media accounts

School social media accounts may be used for many different purposes.

In general, staff should only post updates, messages or otherwise use these accounts when that use is clearly in line with the school's overall objectives.

For instance, employees may use school social media accounts to:

- Respond to enquiries and requests for help
- Share blog posts, articles and other content created by the school
- Share insightful articles, videos, media and other content relevant to the school, but created by others
- Provide followers with an insight into what goes on at the school
- Promote events or initiatives carried out by the schools

Social media is a powerful tool that changes quickly. Employees are encouraged to think of new ways to use it, and to put those ideas to the HT/HOS.

Inappropriate content and uses

School social media accounts must not be used to share or spread inappropriate content, or to take part in any activities that could bring the school in to disrepute.

When sharing an interesting blog post, article or piece of content, staff should always review the content thoroughly, and should not post a link based solely on a headline.

Further guidance can be found below.

Use of personal social media accounts at work

The value of social media

St Bart's CE MAT's Schools recognise that staff's personal social media accounts can generate a number of benefits. For instance:

- Staff can make educational contacts that may be useful to their jobs
- Staff can discover content to help them learn and develop in their role
- By posting about the school, staff can help to build the school's profile online.

As a result, the school is happy for staff to spend a reasonable amount of time using their personal social media accounts at work.

Personal social media rules

Acceptable use:

- Staff may use their personal social media accounts for work related purposes during regular hours, but must ensure that this is for a specific reason e.g. research linked to an educational topic or another school. Social media should not affect the ability of staff to perform their regular duties.
- Use of social media accounts for non-work purpose is restricted to non-work times, such as breaks and during lunch.

Talking about the school:

- Staff should ensure that it is clear that their social media account does not represent St Bart's CE MAT or its schools' views or opinions.
- Staff may wish to include a disclaimer in social media profiles: 'the views expressed are my own and do not reflect the views of my employer.'

Safe, responsible social media use

The rules in this section apply to:

- Any staff using school social media accounts:
- Staff using personal social media accounts during school time.

Users must not:

- Create or transmit material that might be defamatory or incur liability for the school/Trust.
- Post message, status updates or links to material or content that is inappropriate.

- In appropriate content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling or illegal drugs.
- This definition of inappropriate content or materials covers any text, images or other media that could responsibly offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.
- Use social media for any illegal or criminal activities.
- Send offensive or harassing material to others via social media.
- Broadcast unsolicited views on social, political, religious or other non-educational related matters.
- Send or post messages or material that could damage the Trust's image or reputation.
- Interact with other schools in any ways which could be interpreted as being offensive, disrespectful or rude.
- Discuss colleagues, other schools, parents or children without their knowledge or approval.
- Post, upload, forward or link to spam, junk email or chain emails and messages.

Copyright

The Trust respects and operates within copyright laws. Users may not use social media to:

- Publish or share any copyrighted software, media or materials owned by third parties, unless permitted by that third party.
- If staff wish to share content published on another website, they are free to do so if that website has obvious sharing buttons or functions on it.
- Share links to illegal copies of music, films, games or other software.

Security and data protection

Employees should be aware of the security and data protection issues that can arise from using social networks.

Maintain confidentiality

Users must not:

- Share or link to any content or information owned by the school that could be considered confidential or sensitive.
- This might include personal data about pupils and their families and that of staff or the academic data of pupils.

- Share or link to any content or information owned by another school or person that could be considered confidential or sensitive. For example, if another school's academic or personal data was leaked online, staff of St Bart's CE MAT should not mention it on social media.
- Share or link to data in any way that could breach the school's data protection policy.

Protect social accounts

- School social media accounts should be protected by strong passwords that are changed regularly and shared only with authorised users.
- Wherever possible, employees should two-factor authentication (often called mobile phone verification) to safeguard school accounts.
- Staff must not use a new piece of software, app or service with any of the school's social media accounts without receiving approval from the HT/HOS.

Avoid scams

- Staff should watch for phishing attempts, where scammers may attempt to use deception to obtain information relating to either the company or its customers.
- Staff should never reveal sensitive details through social media channels. Identities must always be verified in the usual way before any account information is shared or discussed.
- Staff should avoid clicking links in posts, updates and direct messages that look suspicious. In particular, users should look out for URLs contained in generic or vague-sounding direct messages.

Policy enforcement

Monitoring social media use

School IT and internet resources – including computers, smart phones and internet connections – are provided for legitimate business use.

The company therefore reserves the right to monitor how social networks are used and accessed through these resources.

Any such examinations or monitoring will only be carried out by authorised staff. Additionally, all data relating to social networks written, sent or received through the school's computer systems is part of official records.

The school can be legally compelled to show that information to law enforcement agencies or other parties.

Potential sanctions

Knowingly breaching this social media policy is a serious matter. Users who do so will be subject to disciplinary action, up to and including termination of employment. In this circumstance, the Trust's Disciplinary Policy will be followed.

Staff, contractors and other users may also be held personally liable for violating this policy. Where appropriate, the school will involve police or other law enforcement agencies in relation to breaches in this policy.

Appendix I: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber-attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.

TERM	DEFINITION
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.