Banks St. Stephen's Church of England Primary School

"Belonging, Serving, Succeeding"

Vision for Banks St. Stephen's Church of England Primary School

"We actively promote a sense of pride in belonging to this community. Leading by example, we seek opportunities to serve God by serving others. We are ambitious for each individual and determined to enable every member of the school community to flourish and succeed."

Online Safety Policy

Developing and Reviewing this Policy:

This Online Safety Policy has been written as part of a consultation process involving the following people: Computing Subject Lead, Headteacher, teaching staff and Governors of Banks St Stephen's CE Primary School. It has been approved by Governors and will be monitored and reviewed as listed below:

Policy Created: May 2020

Reviewed: November 2022

The implementation of this policy will be monitored by the Headteacher, back up DSLs and Governors.

Introduction

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2019 (KCSIE) including September 2022 update, 'Teaching Online Safety in Schools' 2019 and other statutory documents and it sits alongside our school's statutory Safeguarding (Child Protection) Policy. Any issues and concerns with online safety must follow our school's safeguarding and child protection procedures. DfE Online Safety in Schools Advice

What are the main online safety risks today?
Online safety risks are traditionally categorised as one of the 3 Cs: Content, Contact or Conduct (identified by Professor Tanya Byron's 2008 report "Safer children in a digital world"). These three areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three. Many of these new risks are mentioned in KCSIE, e.g. fake news, upskirting and sticky design.

How will this policy be communicated?
In order for this policy to impact upon practice it must be accessible and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the school website

- Available on the internal staff network/drive
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff)
- 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.

Aims and Overview

This policy aims to:

- Set out expectations for all Banks St. Stephen's community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform.
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, so that they may survive and thrive online.
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care.
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice.
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession.
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns.

Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, in line with our Safeguarding Policy. The DSL and back-up DSL's (Designated Safeguarding Leads) will handle referrals to local authority multi-agency safeguarding hubs (MASH) and to the LA designated officer (LADO).

Beyond this, https://swgfl.org.uk/online-safety/ has a list of curated links to external support and helplines for both pupils and staff, including the Professionals' Online Safety Helpline from the UK Safer Internet Centre as well as hotlines for hate crime, terrorism and fraud, and anonymous support for children and young people.

Scope

This policy applies to all members of the Banks St. Stephen's community (including staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role

Roles and Responsibilities

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

The Headteacher's Key responsibilities:

- Foster a culture of safeguarding, where online safety is fully integrated into whole-school safeguarding.
- Ensure that the DSL responsibilities listed in the section below are being followed and fully supported.

- Ensure that policies and procedures are followed by all staff.
- Undertake training in accordance with statutory guidance.
- Receive regular updates on school issues and broader policy and practice information.
- Take overall responsibility for data management and information security, ensuring the school's provision follows best practice in information handling; work with the DPO and governors to ensure a GDPR-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.
- 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 cloud systems are implemented according to child-safety first principles.
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
- Ensure that staff are trained in the PREVENT duty.
- Ensure that there is a system in place to monitor and support staff (APEX NS) who carry out internal technical online safety procedures.
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety.
- Ensure the school website meets statutory requirements.

Designated Safeguarding Lead (the Headteacher) and back-up DSL's (Deputy HT, Member of SLT and Pupil Support Manager)

Key responsibilities ***(all quotes below are from Keeping Children Safe in Education 2019)***

- "*The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety*)."
- Ensure "*An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate*."
- "*Liaise with the local authority and work with other agencies in line with Working together to safeguard children.*"
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns.
- Work with the governors to ensure a GDPR-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.
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.
- 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.
- Promote an awareness and commitment to online safety throughout the school community.
- Communicate regularly with Safeguarding Link Governor to discuss current issues (anonymised) and review incident logs (CPOMS)
- 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 – on CPOMS.
- Oversee and discuss 'appropriate filtering and monitoring' with governors and ensure staff are aware of the BTLS filtering that we use.
- Ensure the 2018 DfE guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying.
- Facilitate training and advice for all staff:
    - all staff must read KCSIE Part 1 and all those working with children Annex A
    - it would also be advisable for all staff to be aware of Annex C (online safety)
    - cascade knowledge of risks and opportunities throughout the organisation.

Governing Body, led by Safeguarding Link Governor

Key responsibilities ***(all quotes below are from Keeping Children Safe in Education 2022)***

- 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.
- "*Ensure an appropriate* ***senior member*** *of staff, from the school or college leadership team, is appointed to the role of DSL [with]* ***lead responsibility*** *for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support…"*
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- Have regular strategic reviews with the DSL and incorporate online safety into standing discussions of safeguarding at governor meetings.
- Work with the Data Protection Officer (Deputy Headteacher) and Headteacher to ensure a GDPR-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 A; check that Annex C on Online Safety reflects practice in our school.
- "*Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated […] in line with advice from the local three safeguarding partners […] integrated, aligned and considered as part of the overarching safeguarding approach*."
- "*Ensure appropriate filters and appropriate monitoring systems are in place [but…] be careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding*".
- "*Ensure that children are taught about safeguarding, including online safety […] as part of providing a broad and balanced curriculum […] Consider a whole school or college approach to online safety [with] a clear policy on the use of mobile technology*."

All Staff

Key responsibilities

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up but know who the Designated Safeguarding Lead (DSL) is within their school. The Headteacher is the DSL, Mrs Mussell, Mr Richardson and Mrs Tennant are the back-up DSL's. Mrs S. Robinson is the Safeguarding Link Governor.
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections).
- Read and follow this policy in conjunction with the school's main safeguarding policy.
- Record online safety incidents on CPOMS in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece, so do not keep anything to yourself.
- Sign and follow the staff acceptable use policy and code of conduct.
- Notify the DSL if policy does not reflect practice in your school and use the LCC Whistleblowing Policy if concerns are not promptly acted upon.
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting 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, encourage sensible use, monitor what students are doing and consider potential dangers and the age appropriateness of websites (BTLS provide filtering and monitoring services – more information available at https://education.btlancashire.co.uk/).
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including extra-curricular, home learning and extended school activities if relevant),

supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

- Prepare and check all online source and resources before using within the classroom.
- Encourage pupils/students to follow their acceptable use policy, remind them about it and enforce school sanctions.
- Notify the DSL of new trends and issues before they become a problem.
- Take a zero-tolerance approach to bullying and low-level sexual harassment.
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom.
- Receive regular updates from the DSL and have a healthy curiosity for online safety issues.
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

PSHE Lead

Key responsibilities ***(all quotes below are from Keeping Children Safe in Education 2022)***

As listed in the 'all staff' section, plus:

- Embed consent, mental wellbeing, healthy relationships and staying safe 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*."
- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies. See the Purple Mash Scheme of Work for more detail.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSE and Health education.

Computing Leads

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. See the Purple Mash Scheme of Work for more details.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within computing.
- Collaborate with technical staff (APEX NS) to ensure a common and consistent approach, in line with acceptable-use agreements.

All other Subject Leads

Key responsibilities

As listed in the 'all staff' section, plus:

- Look for opportunities to embed online safety in your subject and model positive attitudes and approaches to staff and pupils alike.

Network Manager/Technicians (APEX NS)

Key responsibilities

As listed in the 'all staff' section, plus:

- 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 DSL (Headteacher) and data protection officer (Deputy Headteacher Mrs Mussell) to ensure that school systems and networks reflect school policy.

- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems.
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team.
- Maintain up-to-date documentation of the school's online security and technical procedures.
- 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.

Data Protection Officer (Deputy Headteacher)
Key responsibilities

- Work with the Headteacher and Governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.

Volunteers, Students and Contractors
Key responsibilities

- Read, understand, sign and adhere to an acceptable use policy (AUP).
- Report any concerns, no matter how small, to the Headteacher.
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviours in their own use of technology.

Pupils
Key responsibilities

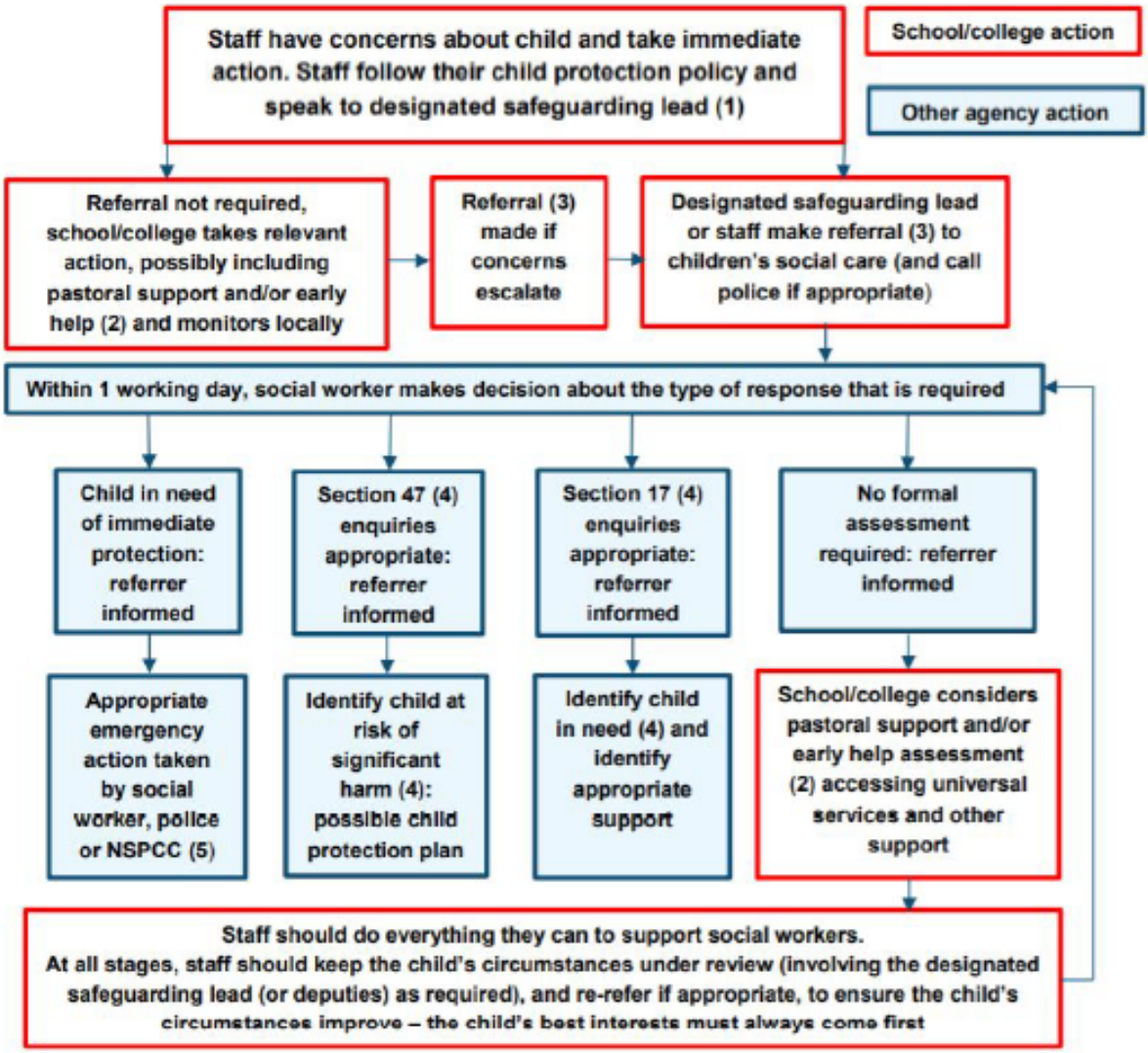
- Read, understand, sign and adhere to the pupil acceptable use policy and review this annually.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials.
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems.

Parents/carers
Key responsibilities

- Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it.
- Consult with the school if they have any concerns about their child's and others' use of technology.
- Promote positive online safety and model safe, responsible 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.

Actions where there are concerns about a child

The following flow chart is taken from page 22 of Keeping Children Safe in Education 2022 as the key education safeguarding document.



(1) In cases which also involve a concern or an allegation of abuse against a staff member, see Part Four of this guidance.

(2) Early help means providing support as soon as a problem emerges at any point in a child's life. Where a child would benefit from co-ordinated early help, an early help inter-agency assessment should be arranged. Chapter one of Working Together to Safeguard Children provides detailed guidance on the early help process.

(3) Referrals should follow the process set out in the local threshold document and local protocol for assessment. Chapter one of Working Together to Safeguard Children.

(4) Under the Children Act 1989, local authorities are required to provide services for children in need for the purposes of safeguarding and promoting their welfare. Children in need may be assessed under section 17 of the Children Act 1989. Under section 47 of the Children Act 1989, where a local authority has reasonable cause to suspect that a child is suffering or likely to suffer significant harm, it has a duty to make enquiries to decide whether to take action to safeguard or promote the child's welfare. Full details are in Chapter one of Working Together to Safeguard Children.

(5) This could include applying for an Emergency Protection Order (EPO).

Handling online-safety concerns and incidents

School procedures for dealing with online safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding (Child Protection) 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).

Banks St. Stephen's commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively.

Any suspected online risk or infringement should be reported to the DSL on the same day.

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). 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, NCA CEOP, Prevent Officer, Police, IWF). 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 disturbing or breaks the law.

Sexting

At Banks St Stephen's we refer to the UK Council for Internet Safety (UKCIS) guidance on sexting in schools. It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

There is a one-page overview called *Sexting; how to respond to an incident* for all staff to read, in recognition of the fact that it is mostly someone other than the DSL to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL. Each schools' DSL will in turn use the full guidance document, *Sexting in Schools and Colleges* to decide next steps and whether other agencies need to be involved.

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying should be treated like any other form of bullying and the school's anti-bullying policy should be followed for online bullying, which may also be referred to as cyberbullying.

Sexual Violence and Harassment

DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education and also a document in its own right. It would be useful for all staff to be aware of this guidance: paragraphs 51-57 cover the immediate response to a report and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture. The guidance stresses that schools must

take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

Misuse of School Technology

Clear and well-communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct. Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Social Media Incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Banks St. Stephen's community. These are also governed by school's Acceptable Use Policies.

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct (for staff). Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, senior leadership will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Data Protection and Data Security

There are references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), which the DPO and DSL will seek to apply. This quote from the latter document is useful for all staff – note the red and purple highlights:

"***GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe.*** *Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need.* ***The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent*** *(DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies)* ***it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children***."

The Headteacher, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions.

Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to "*ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding*."

At Banks St. Stephen's, the internet connection we subscribe to is provided by LCC Education Digital Services and they provide us with a high level filtering service (Netsweeper) and Sophos Anti-Virus software. This means we have a dedicated and secure, school-safe connection that is protected with firewalls and multiple layers of security.

Email

All staff and governors at Banks St. Stephen's have access to Microsoft Office 365 as the preferred school e-mail system. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection. General principles for email use are as follows:

- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.
- Staff are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.
- Governors also have a dedicated school email address used only for governor business

School Website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website to the office administration team. The Headteacher, supported by the governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained. The school website complies with statutory DFE requirements. Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website. Where other staff submit information for the website, they are asked to remember:

- School have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission.
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published.

Cloud Platforms

Banks St. Stephen's adheres to the principles of the DfE document 'https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges'. *Last updated October 2022.*

The data protection officer and technicians analyse and document systems and procedures before they are implemented, and regularly review them. Staff and pupils are expected to keep their passwords safe and secure. The administration of usernames and passwords ensures that staff and governors use the platform safely.

The following principles apply:

- Pupil images/videos are only made public with parental permission.
- Only school-approved platforms are used.
- All stakeholders understand the difference between consumer and education products (e.g. a private email account or cloud platform and those belonging to a managed educational domain).

Digital images and video

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long.

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose. Any pupils shown in public facing materials are never identified with more than first name.

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. Photos are stored on the school network or on school devices in line with the retention schedule of the school Data Protection Policy. Staff use the school iPads to take photos and are not permitted to use their own mobile phones or other personal devices for taking photos of children.

Staff and parents are regularly reminded about the importance of not sharing without permission, due to reasons of child protection, data protection, religious or cultural reasons, or simply for reasons of personal privacy.

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences, which might include governors, parents or younger children.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Social Media

At Banks St. Stephen's we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

The Senior Leadership Team and Computing Subject Lead are responsible for managing our social media accounts.

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there have been 200 Prohibition Orders issued to teachers over the past four years related to the misuse of technology/social media.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video and permission is sought before uploading photographs, videos or any other information about other people.

Device Usage

- **Pupils** in Y6 are, with parental permission, allowed to bring mobile phones because they walk to and from school alone. These devices are kept in the Y6 cupboard at the start of the day and returned at the end. Children are not allowed to use these devices during the school day. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office. We have an internal communication Whatsapp group entitled "Communicating in School" for communicating internal messages for safeguarding reasons e.g. absences and messages from SLT regarding staff meetings etc. All messages are school related and monitored by the Headteacher, SLT and DSLs.
- **Volunteers, students, contractors, governors** should leave their phones in their pockets/bags. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.
- **Parents** should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to the Digital images and video section of this document. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.
- Staff use the school iPads to take photos and never use their own mobiles or other personal devices.

Network / internet access on school devices

- **Pupils** are not allowed networked file access via personal devices.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the Digital images and video section on page and Data protection and data security section on page. Child/staff data should never be downloaded onto a private phone.
- The staff have an in-school communication "Whatsapp" group. All staff working within school are members of this communication group, including SLT. Staff are allowed to keep their mobile phones switched on and available but ONLY for this purpose.
- Only approved devices are allowed to use the wireless system.
- **Parents** have no access to the school network or wireless internet on personal devices.

Trips / events away from school

For school trips/events away from school, teachers may use their personal phone for communication. Where possible, all phone calls should be made via the school office.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher, and staff authorised by the headteacher, have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.