ONLINE SAFETY POLICY

February 2024

This policy should be read in conjunction with the following policies and guidance:

- Safeguarding and Child Protection
- Data Protection
- Keeping Children Safe in Education 2023
- Guidance For Safer Working Practice For Those Working With Children and Young People in Education Settings 2022

INTRODUCTION

Information and Communication Technology (ICT) in the 21st Century is an essential resource to support learning and teaching and plays an important role in the everyday lives of children, young people and adults. As Christians this is something that we can celebrate and enjoy, and as a school, use to arm our young people with the skills to access life-long learning and employment. We acknowledge that the responsible use of ICT brings great benefits to the school and individuals, however there are risks associated with its use. This document aims to set out Bethany School's policy on the acceptable use of ICT including Online Safety, social media, and data security.

At Bethany School, we understand the responsibility to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Online safety is a key part of safeguarding so that young people do not see the internet as a separate part of their lives. The school will ensure that online safety is delivered as part of the curriculum on a regular basis.

We understand that the breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk according to KCSIE 2023:

- **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If we feel any of our pupils, students or staff are at risk, it will be reported to the Anti-Phishing Working Group.

Internet, mobile and digital technologies cover a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of internet, mobile and digital technologies within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- E-mail, Instant Messaging, and chat rooms
- Social Media, including Facebook and X (formerly Twitter)
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies, and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much internet, mobile and digital technologies, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these technologies and that some have minimum age requirements (13 years in most cases).

The School holds personal data on learners, staff, and others to help conduct day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day-to-day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreements (for Staff, Volunteers, Governors and Pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

ONLINE SAFETY ROLES AND RESPONSIBILITIES

Governors

As Online Safety is an important aspect of strategic leadership within the school, the Head Teacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

Online Safety Coordinator

Mrs Sarah Walker (Designated Safeguarding Deputy) is the Online Safety Coordinator for Bethany School. It is the role of the Online Safety Coordinator to keep abreast of current issues and guidance through organisations such as the LEA, CEOP (Child Exploitation and Online Protection) and Childnet. She will disseminate information and train or update other relevant members of staff/Governors as required. She will liaise with relevant members of the SMT in areas of information risk policy and risk assessment and coordinate with the data protection compliance manager in relation to GDPR. As a result, online risks are able to be managed and addressed.

Relevant Responsible person

Mr David Charles holds the role of Relevant Responsible Person and Data Protection Lead in School and should receive reports of incidents or breaches in the first instance.

All staff

All members of the school community have been made aware of who holds these posts. However, it should be clear to all staff that Online Safety and the handling of secured data is everyone's responsibility. Failing to apply appropriate controls to secure data could amount to gross misconduct and even result in legal action.

DATA PROTECTION

This school holds a separate Data Protection Policy, including UK GDPR.

VIRUS PROTECTION, FILTERING AND MONITORING

Bethany School has put in place effective Virus, Firewall and Content Filtering and Monitoring software on school devices and school networks, working together with Datamills UK and in light of guidance from Appropriate Filtering and Monitoring - UK Safer Internet Centre and the KCSIE online safety requirements. Governors review the standards and filtering and monitoring provision at least annually.

Our safeguarding needs are met by implementing the following strategies

- IT use is monitored using the 'cisco umbrella' filtering and monitoring system:
- The school will block harmful and inappropriate content without unreasonably impacting teaching and learning.
- ICT equipment owned or leased by the school may be inspected at any time without prior notice on the authorisation of the Head Teacher.
- Authorised ICT consultants, Datamills UK may monitor and inspect all internet activities which make use of the Bethany School server at any time. Personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards, and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 2018, or to prevent or detect crime.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Virus Protection includes the following

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory will be checked for viruses using the anti-virus software installed on the school ICT network.

If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the ICT support provider immediately (Datamills UK). The ICT support provider will advise you what actions to take and be responsible for advising others who need to know.

BREACHES

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of permission to use school ICT hardware, software or services for a specified period.

For staff, any policy breach is grounds for disciplinary action in accordance with the Staff Code of Conduct and may lead to criminal or civil proceedings.

For pupils, reference will be made to the school's Good Behaviour and Discipline Policy and include reporting the breach to the Head Teacher who may consider a period of exclusion. The Head Teacher may refer the matter to Governors who may take further action.

The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

INCIDENT REPORTING

An 'incident' is taken to mean any event which contravenes the "ICT Acceptable Use Agreement". See Appendix A "Response to an Incident of Concern". These include any security breaches or attempts, loss of equipment or PINs, virus notifications, data breaches and any unauthorised use of suspected misuse of the internet. Mobile and digital technologies

Any incident must be immediately reported to the School's Relevant Responsible Person (Mr David Charles). Incidents may include a security breach or attempted security breach, loss of equipment and any unauthorised use or suspected misuse of the ICT system in relation to data security, accessing inappropriate material, or misuse of emails.

Some incidents may need to be recorded if they relate to bullying, extremism or racist behaviour. This will be via our Incident or Anti-bullying log or the Head Teacher's Behaviour Record and will take into account our Safeguarding, Prevent Strategy, Anti-bullying and Good Behaviour and Discipline Policies.

Please refer to the relevant section on **Incident Reporting, Online-Safety Incident Log & Infringements.**

DATA SECURITY AND ICT ACCEPTABLE USE

The accessing and appropriate use of school data is something that Bethany School takes very seriously with reference to GDPR regulations and Data protection in schools - Guidance - GOV.UK

An Information Asset Register is held which enables us to be aware of what information is stored and for what purposes, as well as how it needs to be protected, how information will be amended or added to over time, who has access to data and why and how information is retained and disposed of. (See Data Protection Policy for more details about the relevant responsible people for data protection).

The school gives relevant staff access to its ICT network when they have been issued with guidance and training and have signed the **ICT Acceptable Use Agreement** to demonstrate that they have understood the school's Online Safety Policy and Data Security issues. See Appendix for A for ICT acceptable use agreements.

All staff are issued with a unique username and password which must always be used and must not be disclosed unless to authorised ICT staff, when necessary.

It is the responsibility of everyone to keep passwords secure and inform the head teacher immediately if there is a breach of security with password or account information.

Personal data must not be downloaded onto storage devices or laptops.

All staff are responsible for keeping school related data secure. This includes all personal, sensitive, confidential or classified data used in school or, when relevant, taken out of school. Staff should be careful with mobile ICT equipment and printed data, especially using shared printers/copiers. They should use the 'delay print function' when printing sensitive data from a device located away from the printer. They should also be aware of sensitive information which may be seen if left open on an unprotected computer screen.

ZOMBIE ACCOUNTS

Zombie accounts' refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access. Bethany School will ensure that all user accounts are disabled once the member of the school has left. Prompt action on disabling accounts and regularly changing generic passwords will avoid unauthorised access.

DISPOSAL OF REDUNDANT ICT EQUIPMENT POLICY

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data
- All redundant ICT equipment that may have held personal data will have the storage media over-written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any ICT equipment will conform to:
  The Waste Electrical and Electronic Equipment Regulations 2006
  The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
  http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
  http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
  http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

  Data Protection Act 2018
  ico education-data

  Electricity at Work Regulations 1989
  http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal
- The school's disposal record will include:
  - Date item disposed of
  - Authorisation for disposal, including verification of software licensing and any personal data* likely to be held on the storage media
  - How it was disposed of e.g., waste, gift, sale
  - Name of person & / or organisation who received the disposed item

* If personal data is likely to be held the storage media will be overwritten multiple times to ensure the data is irretrievably destroyed.

Further information available at:

Waste Electrical and Electronic Equipment (WEEE) Regulations
Regulations: Waste Electrical and Electronic Equipment (WEEE) - GOV.UK
Environment Agency website
Electrical waste: retailer and distributor responsibilities
Information Commissioner Website
ICO
Data Protection Act – data protection guide
UK GDPR guidance and resources | ICO

ONLINE/VIRTUAL TEACHING

If the school needs to use online or virtual teaching the school will:

- ensure all relevant staff are briefed so they understand the policies and the standards of conduct expected of them.
- consider any advice published by the local authority, or their online safety / monitoring software provider.

Whilst using online or virtual teaching staff should:

- adhere to all the usual safeguarding and online safety practices and procedures.

EMAIL

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and how to behave responsible online. In whatever way school e-mails are accessed (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

MANAGING E-MAIL

- The school gives all staff & Governors their own email account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed. Personal email addresses should not be used. If this is not possible (ie parent volunteer), emails should be directed towards the school office email account and forwarded from there.
- Each account holder is responsible for keeping passwords secure
- E-mail should be used responsibly and checked regularly.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- For the safety and security of users and recipients, all mail is filtered and logged, if necessary, e-mail histories can be traced.
- E-mails created or received as part of the school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. Therefore, e-mail accounts must be actively managed as follows:
    - Delete all emails of short-term value.
    - Organise email into folders and carry out frequent housekeeping on all folders and archives
- Attachments from an untrusted source should never be opened;
- Staff must inform the Head Teacher if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of ICT lessons, Tutor Time and particularly during communication Topic.
- Pupils may access their own email account at certain times during school, but are expected to behave responsibly, in line with the ICT Acceptable Use Agreement.
- Pupils in Y6/Y7-Y11 are issued with School email addresses for educational purposes. These accounts will be deleted when the pupil leaves Bethany School.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting e-mail

E-MAILING PERSONAL, SENSITIVE, CONFIDENTIAL OR CLASSIFIED INFORMATION

Emailing sensitive, confidential or classified information is discouraged, however where your conclusion is that email must be used to transmit such data you must liaise with your Head Teacher and exercise caution when sending the email. Documents of this nature should be sent to no more recipients than necessary, as a password protected attachment and details/receipt verified by phone or email. The password must be provided by separate contact with the recipient. Often posting or hand delivering such documents is preferred.

INTERNET USE AND ONLINE SAFETY IN THE CURRICULUM

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas, and publish material which makes it both an invaluable resource for education, business, and social interaction, as well as a potential risk to young and vulnerable people

ICT and online resources are increasingly used across the curriculum. We believe it is essential for online-Safety guidance to be given to the pupils on a regular and meaningful basis. Close attention has been paid to DfE Guidance for teaching online safety in school June 2019.

See Teaching online safety in schools - GOV.UK

and

Education for a Connected World - GOV.UK

In accordance with KCSIE 2023, Bethany school will review its approach to online safety every year using an online safety audit tool such as LGFL online safety audit https://hubs.ly/Q01fRmg00 or https://sheffieldscb.proceduresonline.com/p_online.html

Pupils are taught online safety, computing, ICT, use of e-mail, and internet use throughout the school curriculum including in tutor time, ICT lessons, communication topic and worldview studies. See curriculum grids for more information on areas such as health and wellbeing, sexual exploitation, cyberbullying, gang culture and criminal exploitation, cybersecurity and radicalisation.

Online safety curriculum content includes.

- Accessing designated websites under supervision, with permission (for pre checked, designated sites) or independently (for senior age pupils when the Acceptable Use Agreement has been signed.)
- Educating pupils about the online risks that they may encounter outside school in an age-appropriate manner informally when opportunities arise
- Reception and Y1 consider online safety in PSHE. Junior pupils complete the ‘internet legends’ internet safety course from Google, and pupils in Y2 upwards have Online Safety lessons in their computing lessons or tutor time at the start of the academic year. Secondary pupils will complete an individual certificate of online safety via https://www.onlinesafetyalliance.org/ in the senior class and then again in the GCSE class. Pupils in Year 7 upwards will be expected to sign the ICT Acceptable Use Agreement each year, and are regularly reminded of its contents during tutor time and via poster displays
- Pupils are taught about copyright, respecting other people’s information, safe use of images and not sharing personal details through discussion, modelling and appropriate activities within the classroom
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience

problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member or an organisation such as Cybermentors, Childline or CEOP report abuse button.

- Pupils are taught to critically evaluate materials and learn good searching skills throughout the curriculum.
- Online Safety advice is promoted widely through school displays, posters and class activities such as Safer Internet Day in February.
- Some aspects of Online Safety are covered when every Year 6 group attends the “Crucial Crew” event run by South Yorkshire Police.

EQUAL OPPORTUNITIES: PUPILS WITH ADDITIONAL NEEDS

The school endeavours to create a consistent message with parents for all pupils however, staff should be aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues.

Where a pupil has poor social understanding, careful consideration should be given to group interactions when raising awareness of e-Safety. Internet activities should be planned and well managed for these children and young people.

Updates - Meeting digital and technology standards in schools and colleges - Guidance - GOV.UK

ONLINE SAFETY SKILLS DEVELOPMENT FOR STAFF

New staff receive information on the School’s Online Safety policy and ICT Acceptable Use Agreement as part of their induction. Some staff have completed the ‘Internet legends’ training course provided by Google and all staff access annual training from https://www.onlinesafetyalliance.org.

All staff are made aware of their individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community (report to the Head Teacher). As this policy is reviewed, staff are made aware of changes and are regularly reminded of their responsibilities.

All staff are encouraged to incorporate Online Safety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern at regular staff meetings.

INCIDENT REPORTING AND RECORDING

An ‘incident’ is taken to mean any event which contravenes the “ICT Acceptable Use Agreement”. See Appendix B “Response to an Incident of Concern”.

Any incident must be immediately reported to the School’s Relevant Responsible Person (Mr David Charles). Incidents may include a security breach or attempted security breach, loss of equipment (including remote access ID and PINs), and any unauthorised use or suspected misuse of the ICT system in relation to data security, accessing inappropriate material, or misuse of emails.

Some incidents may need to be recorded if they relate to bullying, extremism or racist behaviour. This will be via our Incident or Anti-bullying log or the Head Teacher’s Behaviour Record and will take into account our Safeguarding, Prevent Strategy, Anti-bullying and Good Behaviour and Discipline Policies.

INAPPROPRIATE MATERIAL

Please see the guidance below regarding how to respond to an incident involving a **nude or semi-nude image** of a child/pupil. **Never** view, copy, print, share, store or save the imagery yourself, or ask a child to share or download – **this is illegal**. If you have already viewed the imagery by accident (e.g. if a young person has shown it to you before you could ask them not to), report this to the DSL (or equivalent) and seek support.

Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK

- All users are aware of the procedures for reporting accidental access to inappropriate materials. If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the Head Teacher, or teacher as appropriate

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Head Teacher. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of the LADO and police for very serious offences

- Users are made aware of sanctions relating to misuse or misconduct in the code of conduct and safeguarding policies.

MANAGING OTHER ONLINE ISSUES

Online technologies (including social networking sites, if used responsibly can provide easy to use, creative, collaborative, and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some **content, contact, culture, and commercialism**. (The four areas of online safety risk, KCSIE) To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- All pupils are required to keep their mobile phones switched off and in their bags for the duration of the school day including before school

- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are

- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online, including images, and address/location information

- Our pupils are asked to report any incidents of Cyberbullying to their teacher or the Relevant Responsible Person, Mr David Charles

- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored https://www.saferinternet.org.uk/blog/age-restrictions-social-media-services

- Please see our "Social Media Responsible Use Guidelines" in Appendix B which give more detailed advice about using good judgement and being respectful and responsible when representing Bethany School in Social Media Spaces

- On-line gambling or gaming is not allowed.

- Staff wil preview recommended sites, online services, software and apps before use.

PARENTAL INVOLVEMENT

We believe that it is essential for parents/carers to be fully involved with promoting e-Safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss e-Safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain, specifically in printed material, display material, school website, Bethany School public Facebook page, parents and teachers Facebook page. They are also expected to adhere to the decision made by other parents in this regard and not assume that consent has been given when taking and sharing images themselves

- Parents/carers of Senior pupils are expected to sign The Pupil ICT Acceptable Use Agreement with their children

- Volunteer helpers are expected to sign the Staff/Governors/Volunteers ICT Acceptable Use Agreement

- Bethany School disseminates information to parents relating to online safety where appropriate through:

  - Parents meetings
  - Practical training session's e.g. current online safety issues, and online safety training for parents from https://www.onlinesafetyalliance.org/.
  - Monthly email newsletters from 'Knowsley City Learning Centres' Online Safety - Knowsley City Learning Centres

PERSONAL OR SENSITIVE INFORMATION

PROTECTING PERSONAL, SENSITIVE, CONFIDENTIAL AND CLASSIFIED INFORMATION

Personal, sensitive or confidential information must be processed in accordance with the schools data protection policy

- Ensure that any school information accessed from a personal PC or removable media equipment is kept secure and any portable media is removed from computers when not attended.
- Ensure screens are locked before moving away from computers during a normal working day to prevent unauthorised access.
- Ensure the accuracy of any personal, sensitive, confidential, and classified information that is disclosed or shared with others.
- Ensure that personal, sensitive, confidential, or classified information is not disclosed to any unauthorised person.
- Ensure the security of any personal, sensitive, confidential, and classified information contained in documents that are copied, scanned, or printed. This is particularly important when shared copiers (multi-function print, scan, and copiers) are used.
- Only download personal data from systems if expressly authorised to do so
- Personal, sensitive, confidential, or classified information must not be posted on the internet, or such information disseminated in any way that may compromise its intended restricted audience.
- Screen displays must be kept out of direct view of any third parties when accessing personal, sensitive, confidential, or classified information.
- Hard copies of data must be securely stored and disposed of after use in accordance with the document labelling.

STORING/TRANSFERRING PERSONAL, SENSITIVE, CONFIDENTIAL OR CLASSIFIED INFORMATION USING REMOVABLE MEDIA

- Removable media should be purchased with encryption.
- All removable media must be stored securely.
- All removable media that may hold personal data must be securely disposed of.
- All files containing personal, sensitive, confidential, or classified data must be encrypted.
- Hard drives from machines no longer in service must be removed and stored securely or wiped clean.

  Guidance on How to Encrypt Files can be found on the ICO website:
  https://ico.org.uk/media/for-organisations/encryption-1-0.pdf

REMOTE ACCESS

- Staff members are responsible for all activity via their remote access facility.
- Any equipment must be used with an appropriate level of security for remote access.
- To prevent unauthorised access to school systems, all dial-up access information such as telephone numbers, logon IDs and PINs must be kept confidential and not disclosed to anyone.
- PINs must be selected to ensure that they are not easily guessed, e.g., do not use personal house or telephone numbers or choose consecutive or repeated numbers.
- Writing down or otherwise recording any network access information must be avoided. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.
- School information and data must be protected, including any printed material produced while using the remote access facility. Particular care must be taken when access is from a non-school environment.

SAFE USE OF IMAGES

TAKING OF IMAGES AND FILM

The following applies to all parts of the school including the Early Years and Reception class.

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. Guidance can be found at:

https://www.safeguardingsheffieldchildren.org/assets/1/photographs_videos_and_images_sept_22.pdf

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment and, with due precautions, and with specific permission from the Head Teacher, on personal devices. If images are taken on personal devices, they should be quickly uploaded onto the school system and deleted from the device.

Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the appropriate teacher. Pupils and staff must have permission from the Head Teacher before any image can be uploaded for publication.

CONSENT OF ADULTS WHO WORK AT THE SCHOOL

Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

PUBLISHING PUPIL'S IMAGES AND WORK

On a child's entry to the School, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the School website
- in the School prospectus and other printed publications.
- in display material that may be used within the School.
- on the School's public Facebook page
- on the School's private "parents and teachers Facebook page"

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the School.

Pupils' full names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Further information relating to issues associated with school websites and the safe use of images in schools may be found at:

[Data protection and school websites - Hertfordshire Grid for Learning]

STORAGE OF IMAGES

In line with GDPR, images are used only with the written consent of the parent/carer, which is secured in the first instance on a child's entry to school. Records are kept on file and consent can be changed by parents/carers at any time.

Specific additional consent is gained for the use of images in the pupil learning record for reception pupils only.

Images/ films of children are stored securely on the school's network and deleted once the pupils has left unless consent is gained to use the image, e.g. in publicity material.

Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks or smart phones) without the express permission of the Head Teacher.

In the Early Years setting images are taken on the classroom camera, which is stored securely, and then removed to the class computer weekly. The class teacher has the responsibility of deleting the images when they are no longer required, or when the pupil has left the School.

WEBCAMS and VIDEO CONFERENCING

- We do not use publicly accessible webcams in school.
- Permission will be sought from parents and carers if their children are involved in video conferences with endpoints outside of the school.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document).
- Webcams include any camera on an electronic device which is capable of producing video. School policy should be followed regarding the use of such personal devices.
- Additional points to consider:
- Participants in conferences offered by 3rd party organisations may not be DBS checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

MOBILE TECHNOLOGIES

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such as smartphones, tablets, and games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

PERSONAL MOBILE DEVICES (INCLUDING MOBILE PHONES)

- The school allows staff to bring in personal mobile phones and devices for their own use, generally outside of lesson time.

- Pupils are allowed to bring personal mobile devices/phones to school but must not use them at any time during the school day including break times and before and after school. Mobile phones should be switched off and kept in a pupils bag, phones seen out during the school day will be confiscated. Occasionally pupils may be given permission to use mobile phones for research purposes with the express permission of their class teacher.
- All adults in school (teachers, volunteers, parent helpers etc.) are encouraged to demonstrate good practice by not using their own mobile phone for personal reasons in front of the children. There may be occasions where it is appropriate for an adult to use a mobile phone or similar device, for instance calling for assistance or use multi-factor authentication.
- The school is not responsible for the loss, damage, or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Never use a hand-held mobile phone whilst driving a vehicle.
- The School has a digital camera and mobile telephone which is available for use by staff during off site School trips for making calls and taking photos which can then be uploaded to the School system.

SOCIAL MEDIA

Facebook, Twitter, Instagram and other forms of social media are increasingly becoming an important part of our daily lives. We use images of families, work and pupils from time to time to publicise our School on our Facebook page and website, when appropriate consent has been obtained. Families may change their consent at any time and ask for images to be removed if desired.

Our School also uses an informal ‘parents and teachers’ Facebook page to communicate with parents and carers. Any parent/staff member is able to post messages to each other and is expected to behave in a respectful and responsible manner in this setting.

The following guidance is sent to all new members of this Facebook group, as part of the group description and is re-posted from time-to-time as a reminder to all parents.

> “I have added you on to the Bethany parents and teachers Facebook group. It's a closed group for us only and we use it for informal reminders, support, requests and sharing information etc. Photos and posts are shared privately within this group on the understanding that they are not re-posted or shared externally without permission from those concerned. Users should be aware that not all pupils have given consent for their images to be posted to this group. They should be considerate of others’ wishes in this regard, and only post images to this group if certain that consent has been given. Seek advice from admin if you are not sure, or ask permission directly.

See **Appendix C** for the Bethany School Social Media Responsible Use Guidelines.

- Staff, Governors, pupils, parents, and carers are aware that the information, comments, images, and videos they post online can be viewed by others, copied, and stay online forever.

- Staff, Governors, pupils, parents, and carers are aware that their online behaviour should always be compatible with UK law.

SERVERS

The Bethany School Server is located in a secure room, accessed by authorised staff only, and all data is regularly backed up off site by Datamills UK.

1. Always password protect and lock the server

2. Existing servers should have security software installed appropriate to the machine's specification
3. Backup tapes should be encrypted by appropriate software
4. Backup tapes/discs must be securely stored in a fireproof container
5. Back up media stored off-site must be secure

WRITING AND REVIEWING THIS POLICY

STAFF AND PUPIL INVOLVEMENT IN POLICY CREATION

Staff and Governors, have been involved in making/ reviewing the ICT Acceptable Use Agreements through **discussion at staff and governors meetings.**

REVIEW PROCEDURE

There will be on-going opportunities for staff to discuss with the Online-Safety coordinator any Online-Safety issue that concerns them.

There will be on-going opportunities for staff to discuss with the DPCM any issue of data security that concerns them.

This policy will be reviewed every (12) months and consideration will be given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted, or the Central Government changes the orders or guidance in any way.

The policy has written with regard to 'Mobile phones in schools - Guidance for schools on prohibiting the use of mobile phones throughout the school day, February 2024'.

https://www.gov.uk/government/publications/mobile-phones-in-schools

This policy has been read, amended, and approved by the staff, Headteacher and Governor

Policy agreed by Governors - 05/02/2024 (revised 10/06/24)

Policy due for Review - January 2025

Appendix A - Bethany School Pupil ICT Acceptable Use Agreement and Online Safety Rules

All of the points in the list on the page below can be summarised as follows:

Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device, as you would face to face.

‘So in everything, do to others what you would have them do to you’ Matthew 7v12

- I will only use school ICT and my school email address for school purposes and not to access chat rooms/personal websites or social media
- I will only access sites which are appropriate for use in school on school equipment, and wont access games, chat rooms or personal websites.
- I will not download or install software on school technologies
- I will only open e-mail attachments from people I know, or who my teacher has approved
- I will only log on to the school network using my own username and password and will not tell other people my ICT passwords
- I will remember to log out when my session has finished
- I will only open/delete my own files
- I will make sure that all ICT contact with pupils, teachers or others is responsible, polite and sensible
- I will not look for, download, save or send anything that is unpleasant or nasty, or is illegal. If I accidentally find anything like this I will report it to my teacher immediately
- I will not give out any personal information such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher
- I am aware that if I take images or video of pupils and/or staff that I must only store and use these for school purposes in line with school policy, and must never distribute or ‘share’ images without the permission of all parties involved. I will not upload any video, images, sounds or text that could upset any member of the school community.
- I will be responsible for my behaviour when using ICT and will try to ensure that my online activity both in school and outside school will not cause distress to others or bring the school community into disrepute.
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
- I will not sign up to online social media sites such as Facebook, Instagram, YouTube, Snapchat etc without permission from my parents
- I will take due care with all school ICT equipment
- I will respect the privacy and ownership of others’ work online at all times
- I will only use my own mobile phone within the rules and understand that my phone will be confiscated if seen outside of these times.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted

Bethany School Pupil ICT Acceptable Use Agreement and Online Safety Rules

Dear Parent/Carer
ICT, including the internet and other communication technologies have become integral to the lives of young people in society and can be powerful tools, opening opportunities for everyone. ICT and safe access to the internet is an important part of education and learning in our school. We expect all children to be safe and responsible when using ICT and not accidentally or deliberately misuse the school systems. Bethany school undertakes to follow every reasonable precaution, including monitoring and filtering systems to ensure that pupils will be kept safe when they use the school internet and ICT systems, however cannot ultimately be held responsible for the nature and content of materials accessed on pupils own mobile devices.

The Online Safety Rules (see over page) have been discussed with your child in School. Please re-read and discuss these Online Safety rules with your child, and return the slip at the bottom of this page to their class teacher. This agreement outlines both your own, and your child's willingness to support the Schools approach to ICT. If you have any concerns or would like some further explanation please contact Mrs Sarah Walker and/or refer to the Online Safety Policy that can be found in the policies section of the school website.

Bethany school endeavours to take every reasonable precaution to ensure that our pupils are safe when using the internet. Please take care to ensure that appropriate systems are also in place at home to protect and support your child/ren. You will find help with this in the online safety newsletter that is circulated via email each month.

Parent Agreement
This document has been discussed with …………………………………………. (Child's name) at home.
I give permission for my child to have access to the internet and ICT systems at school, and be given their own email address for use with google classrooms.
I agree to support the safe use of ICT at Bethany School by helping my child to follow the rules overleaf.
I understand the school's policy is that pupils should not sign up to services such as Facebook, Instagram, Snapchat and YouTube whilst they are under age, (13+ years in most cases, and 16+ for Whatsapp).
I will behave responsibly and respectfully in my own online activity, ensuring that it does not bring the school community into disrepute.
Parent/ Carer Signature ……..……………………..…………………………………… Date……………………

Pupil Agreement
I have discussed the rules overleaf in class and with my parent/carer and agree to abide by them. I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted.

Pupil Signature…………………………………………Class ………………………… Date…………

Bethany School Staff/Governor/Volunteer Acceptable Use Agreement and Online Safety Rules

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in School. This agreement is designed to ensure that all staff are aware of their professional responsibilities, can stay safe online and protect the schools system and data when using any form of ICT. All staff and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs Sarah Walker.

- I understand that the school digital technology systems are intended for educational use within the policies and rules set down by the school
- I will communicate with pupils, parents and other staff using official school systems for school related business.
- I will comply with ICT and google for education security settings such as 2 factor authentication, 6 character pin codes, and secure passwords not disclose passwords to others.
- I will ensure that all electronic communications with pupils and staff are respectful and compatible with my professional role
- I will use the staff WhatsApp group and parent/staff Facebook group appropriately, not for reporting or discussing specific pupil information
- I will follow requirements for data protection as outlined in the online safety and data protection policies to ensure that personal data is kept secure and is used appropriately, whether in School, taken off the school premises or accessed remotely. Personal data can only be taken out of School or accessed remotely when authorised by the Head Teacher
- I will not browse, download, upload or distribute any material that is illegal
- I will immediately report any illegal, inappropriate, or harmful material or incident I become aware of to the appropriate person
- Images of pupils and/or staff/Governors will only be taken, stored and used for professional purposes in line with School policy and with written consent of the parent, carer, Governor or staff member. I will not use personal equipment to take/record images without permission.
- Images will not be distributed outside the School network without the permission of the parent/ carer, Governor, member of staff or Head Teacher and it will not be possible to identify by name, or other personal information those who are featured.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Head Teacher
- I will respect copyright and intellectual property rights and will not access other users files without permission
- I will ensure that my online activity, both in School and outside School, is responsible and respectful and will not bring the School, my professional reputation, or the school community into disrepute
- I will support and promote the School’s online Safety and Data protection policies and help pupils to be safe and responsible in their use of ICT and related technologies
- When using my own mobile device to access school data I will follow the rule set out in the agreement and I will ensure that such devices are protected by up to date software and secure passwords, and ensure that I log out of shared devices to keep data secure and will not download data onto my own device.

User Signature

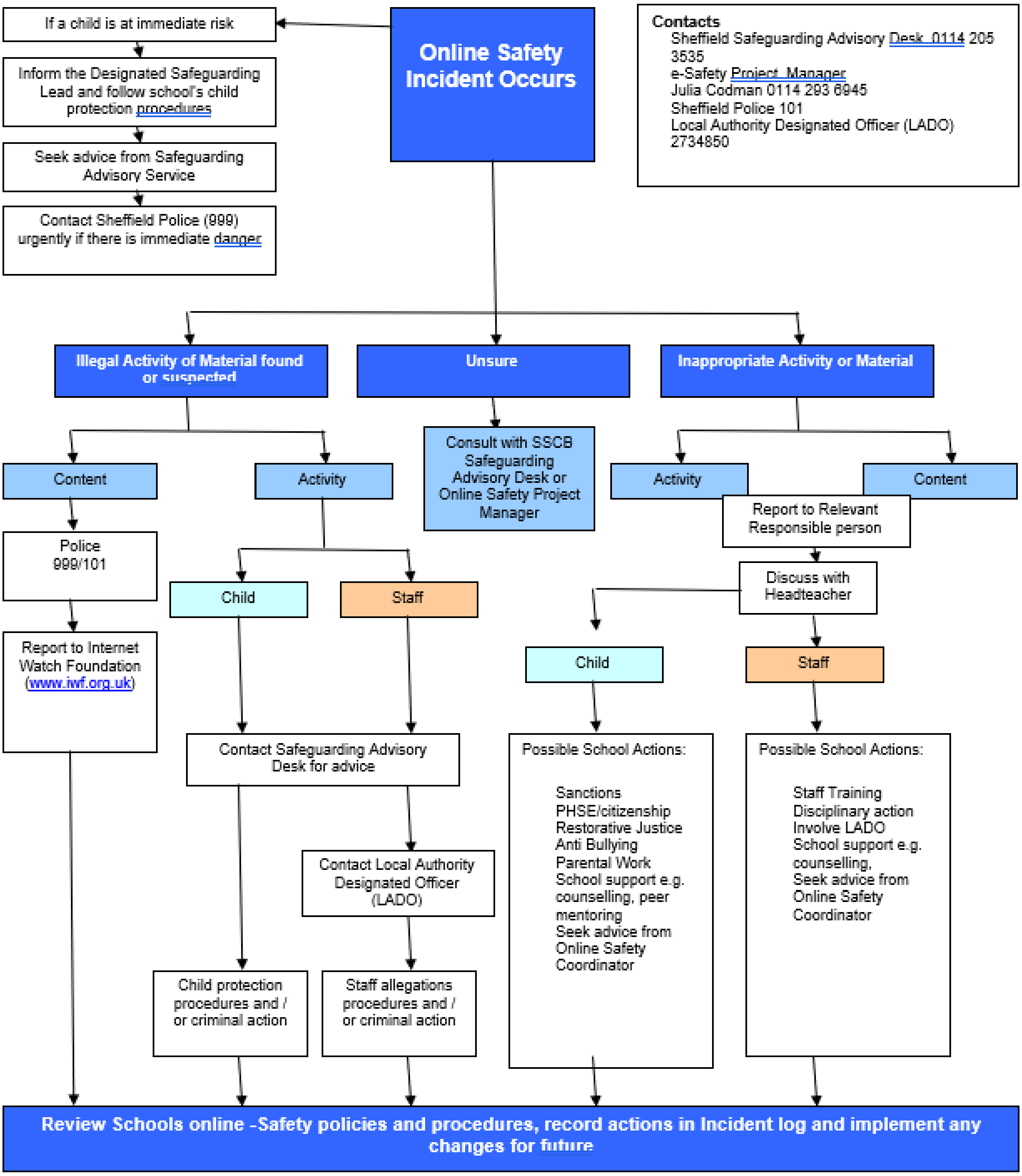
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the School

Signature ……..……………………………… Date ……………………

Full Name …………………………………....................................... (Printed)

Job title ……………………………………………………………………

Appendix B
Response to an Incident of Concern



Online Safety Incident Occurs

If a child is at immediate risk

Inform the Designated Safeguarding Lead and follow school's child protection procedures

Seek advice from Safeguarding Advisory Service

Contact Sheffield Police (999) urgently if there is immediate danger

Contacts
Sheffield Safeguarding Advisory Desk 0114 205 3535
e-Safety Project Manager
Julia Codman 0114 293 6945
Sheffield Police 101
Local Authority Designated Officer (LADO) 2734850

Illegal Activity of Material found or suspected

Unsure

Inappropriate Activity or Material

Content

Activity

Consult with SSCB Safeguarding Advisory Desk or Online Safety Project Manager

Activity

Content

Police 999/101

Child

Staff

Report to Relevant Responsible person

Discuss with Headteacher

Report to Internet Watch Foundation (www.iwf.org.uk)

Child

Staff

Contact Safeguarding Advisory Desk for advice

Possible School Actions:

Sanctions
PHSE/citizenship
Restorative Justice
Anti Bullying
Parental Work
School support e.g. counselling, peer mentoring
Seek advice from Online Safety Coordinator

Possible School Actions:

Staff Training
Disciplinary action
Involve LADO
School support e.g. counselling,
Seek advice from Online Safety Coordinator

Contact Local Authority Designated Officer (LADO)

Child protection procedures and / or criminal action

Staff allegations procedures and / or criminal action

Review Schools online -Safety policies and procedures, record actions in Incident log and implement any changes for future

Appendix C

Bethany School Social Media Responsible Use Guidelines

At Bethany School, teachers, pupils, staff, Governors and parents can use social networking/media (Twitter, Facebook, blogs, etc.) as a way to connect with others, share resources, create educational content, enhance the classroom experience, and network within and outside of the School community. While social networking is fun and valuable, there are some risks we need to keep in mind when using these tools. In the social media world, the lines are often blurred between what is public or private, personal or professional.

Social media refers to online tools and services that allow any Internet user to create and publish content. Many of these sites use personal profiles where users post information about themselves. Social media allows those with common interests to share content easily, expanding the reach of their ideas and work. Popular social media tools include Facebook, Twitter, LinkedIn, blogs, YouTube and Flickr to name a few. Below are guidelines to follow when we are representing Bethany School in social media spaces, regardless of whether these are considered professional or personal spaces.

Use good judgement

We expect good judgement in all situations. Behave in a way that will make you and others proud and reflect well on our School.
Know and follow the School's key values of Respect and Responsibility and our ICT Acceptable Use Agreement.
Regardless of your privacy settings, assume that all of the information you have shared on your social network is public information.

Be respectful
Always treat others in a respectful, positive, and considerate manner.

Be responsible and ethical
Because you represent the School, please stick to discussing only those School-related matters that are within your area of responsibility.
Adults should be open about their affiliation with the School and the role/position they hold.
Share and interact in a way that will enhance your reputation, the reputation of others, and the reputation of the School, rather than damage them.
If you are someone's peer, interact with them online if you are so inclined. If you are a teaching staff member thinking about interacting with a pupil, you are advised to use your School email account and only contact the pupil regarding official School matters. As per the Bethany School staff code of conduct, staff are encouraged not to become "friends" with a current pupil online. If you are uncertain how to proceed, consult the Head Teacher.

Be accurate and appropriate
Check all work for correct use of grammar and spelling before posting.
A significant part of the interaction on blogs, Twitter, Facebook, and other social networks involves passing on interesting content or sharing links to helpful resources. However, never blindly repost a link without looking at the content first

Be a good listener
Keep in mind that one of the biggest benefits of social media is that it gives others another way to talk to you, ask questions directly, and share feedback.
Be responsive to others when conversing online. Provide answers, thank people for their comments, and ask for further feedback.

And if you don't get it right……

Be sure to correct any mistake you make immediately, and make it clear what you've done to fix the mistake.
Apologise for the mistake if the situation warrants it.
If it's a major mistake or data breach (e.g., exposing private information or reporting confidential information), please tell the Head Teacher immediately so the School can take the proper steps to help minimise the impact it may have.

Be confidential
Do not publish, post, or release information that is considered confidential or private. Online "conversations" are never private.
Use caution if asked to share your birth date, address, and mobile/telephone number on any website.

Respect private and personal information
To ensure your safety, be careful about the type and amount of personal information you provide.

- Avoid talking about personal schedules or situations.
- Never share or transmit personal information of pupils, parents, staff, Governors or colleagues online.
- While taking care when posting to safeguard people's privacy, be sure – as necessary and appropriate – to give proper credit to sources. In cases of doubt, privacy should be the default.
- Generally use only first names.
- Always respect the privacy of School community members.
- Post images with care
- Respect brand, trademark, copyright information and/or images of the school.
- Do not caption photos with the names of pupils.
- Do not post photos of pupils who have not given consent to do so. (Ask your teacher or see the Head Teacher for details.)
-

Responding to negative feedback
If someone posts a critique about Bethany School on social media, we hope that a member of our community would respond to the comment in a positive way. The first step is to inform the Head Teacher so the situation can be monitored. The next step is to make contact offline and respond to the comment in a positive way. Our third step would be to have the School respond in an official capacity and if appropriate, suggest a meeting in person to address the issue mentioned in the comment.
If the comment includes profanity, hate speech, or verbally attacks a specific person or group, we delete the comment immediately. Our rationale is that a comment of this sort goes against our view of Responsibility and of Respect and will not be part of Bethany School.

Community of Respect
The most essential standard of appropriate behaviour is that all members of the community will treat one another with kindness, honour, and respect in all situations.

APPENDIX D - HELP AND SUPPORT

Useful Links

Sheffield Safeguarding Partnership Website : Online-Safety

Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK

Information Commissioner's Office https://ico.org.uk/

Sheffield Schools and settings can consult with the e-Safety Manager via: julia.codman@sheffield.gov.uk or telephone 0114 2736945.

Advice on e-Safety - Online safety - Hertfordshire Grid for Learning

Training is available via Safeguarding Training Service on: 0114 2735430 or email safeguardingchildrentraining@sheffield.gov.uk

The UK Safer Internet Centre's Professional Online Safety Helpline offers advice and guidance around e-Safety for professionals who work with children and young people in the UK. The helpline provides support with all aspects of digital and online issues such as social networking sites, cyber-bullying, sexting, online gaming and child protection online. Staff can contact the helpline via 0844 381 4772, helpline@saferinternet.org.uk or can visit www.saferinternet.org.uk/helpline for more information.

"Safer Use of New Technology" is a Kent Safeguarding Children Board (KSCB) document which discusses ideas and FAQs for professionals on how to use technology safely when working with young people. The document can be downloaded from www.kenttrustweb.org.uk?esafety

"Supporting School Staff" is an essential document to help staff understand how to protect themselves online created by Childnet International and DfE: http://www.digizen.org/resources/school-staff.aspx

360 Degree Safe tool is an online audit tool for schools to review current practice: 360 Degree Safe

"Guidance for Safer Working Practice for Adults who Work with Children and Young People" (2009) contains useful guidance around professional use of technology. www.childrenengland.org.uk/upload/Guidance%20.pdf

Further guidance - GDPR, data protection and Freedom of Information (FOI) - Hertfordshire Grid for Learning

CURRENT LEGISLATION

ACTS RELATING TO MONITORING OF STAFF EMAIL

Data Protection Act 2018

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individual's rights of access to their personal data, compensation, and prevention of processing. The **Data Protection Act 2018** implements the UK General Data Protection Regulation (GDPR) in national law.

http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

https://www.legislation.gov.uk/ukpga/2000/23

Human Rights Act 1998

https://www.legislation.gov.uk/ukpga/1998/42

OTHER ACTS RELATING TO ESAFETY

Racial and Religious Hatred Act 2006

It is a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing, or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality, or ethnic background.

http://www.legislation.gov.uk/ukpga/2006/1

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos, or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of *Working Together to Safeguard Children, 2018* document as part of their child protection packs.

https://www.legislation.gov.uk/ukpga/2003/42

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene, or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent there is no need to prove any intent or purpose.

http://www.legislation.gov.uk/ukpga/2003/21/section/127

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

https://www.legislation.gov.uk/ukpga/1990/18

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

https://www.legislation.gov.uk/ukpga/1988/27

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film, and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

https://www.legislation.gov.uk/ukpga/1988/48

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing, or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

https://www.legislation.gov.uk/ukpga/1986/64

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

https://www.legislation.gov.uk/ukpga/1978/37

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

https://www.legislation.gov.uk/ukpga/Eliz2/7-8/66 and http://www.legislation.gov.uk/ukpga/1964/74

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other to fear on each of those occasions.

https://www.legislation.gov.uk/ukpga/1997/40

ACTS RELATING TO THE PROTECTION OF PERSONAL DATA

Data Protection Act 2018

http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

The Freedom of Information Act 2000

https://www.legislation.gov.uk/ukpga/2000/36

https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

COUNTER-TERRORISM AND SECURITY ACT 2015 (PREVENT), ANTI-RADICALISATION & COUNTER-EXTREMISM GUIDANCE

https://www.gov.uk/government/publications/preventing-extremism-in-schools-and-childrens-services

The school holds the document '*The Prevent duty Departmental Advice for Schools and Childcare Providers, June 2015*' on file.

Appendix C

Bethany School Social Media Responsible Use Guidelines

At Bethany School, teachers, pupils, staff, Governors and parents can use social networking/media (Twitter, Facebook, blogs, etc.) as a way to connect with others, share resources, create educational content, enhance the classroom experience, and network within and outside of the School community. While social networking is fun and valuable, there are some risks we need to keep in mind when using these tools. In the social media world, the lines are often blurred between what is public or private, personal or professional.

Social media refers to online tools and services that allow any Internet user to create and publish content. Many of these sites use personal profiles where users post information about themselves. Social media allows those with common interests to share content easily, expanding the reach of their ideas and work. Popular social media tools include Facebook, Twitter, LinkedIn, blogs, YouTube and Flickr to name a few. Below are guidelines to follow when we are representing Bethany School in social media spaces, regardless of whether these are considered professional or personal spaces.

Use good judgement

We expect good judgement in all situations. Behave in a way that will make you and others proud and reflect well on our School.
Know and follow the School's key values of Respect and Responsibility and our ICT Acceptable Use Agreement.
Regardless of your privacy settings, assume that all of the information you have shared on your social network is public information.

Be respectful

Always treat others in a respectful, positive, and considerate manner.

Be responsible and ethical

Because you represent the School, please stick to discussing only those School-related matters that are within your area of responsibility.
Adults should be open about their affiliation with the School and the role/position they hold.
Share and interact in a way that will enhance your reputation, the reputation of others, and the reputation of the School, rather than damage them.
If you are someone's peer, interact with them online if you are so inclined. If you are a teaching staff member thinking about interacting with a pupil, you are advised to use your School email account and only contact the pupil regarding official School matters. As per the Bethany School staff code of conduct, staff are encouraged not to become "friends" with a current pupil online. If you are uncertain how to proceed, consult the Head Teacher.

Be accurate and appropriate

Check all work for correct use of grammar and spelling before posting.
A significant part of the interaction on blogs, Twitter, Facebook, and other social networks involves passing on interesting content or sharing links to helpful resources. However, never blindly repost a link without looking at the content first

Be a good listener

Keep in mind that one of the biggest benefits of social media is that it gives others another way to talk to you, ask questions directly, and share feedback.
Be responsive to others when conversing online. Provide answers, thank people for their comments, and ask for further feedback.

And if you don’t get it right……

Be sure to correct any mistake you make immediately, and make it clear what you’ve done to fix the mistake.

Apologise for the mistake if the situation warrants it.

If it’s a major mistake or data breach (e.g., exposing private information or reporting confidential information), please tell the Head Teacher immediately so the School can take the proper steps to help minimise the impact it may have.

Be confidential

Do not publish, post, or release information that is considered confidential or private. Online “conversations” are never private.

Use caution if asked to share your birth date, address, and mobile/telephone number on any website.

Respect private and personal information

To ensure your safety, be careful about the type and amount of personal information you provide.

- Avoid talking about personal schedules or situations.
- Never share or transmit personal information of pupils, parents, staff, Governors or colleagues online.
- While taking care when posting to safeguard people’s privacy, be sure – as necessary and appropriate – to give proper credit to sources. In cases of doubt, privacy should be the default.
- Generally use only first names.
- Always respect the privacy of School community members.
- Post images with care
- Respect brand, trademark, copyright information and/or images of the school.
- Do not caption photos with the names of pupils.
- Do not post photos of pupils who have not given consent to do so. (Ask your teacher or see the Head Teacher for details.)
-

Responding to negative feedback

If someone posts a critique about Bethany School on social media, we hope that a member of our community would respond to the comment in a positive way. The first step is to inform the Head Teacher so the situation can be monitored. The next step is to make contact offline and respond to the comment in a positive way. Our third step would be to have the School respond in an official capacity and if appropriate, suggest a meeting in person to address the issue mentioned in the comment.

If the comment includes profanity, hate speech, or verbally attacks a specific person or group, we delete the comment immediately. Our rationale is that a comment of this sort goes against our view of Responsibility and of Respect and will not be part of Bethany School.

Community of Respect

The most essential standard of appropriate behaviour is that all members of the community will treat one another with kindness, honour, and respect in all situations.