eSafety & Data Protection Policy

BEDWELL PRIMARY SCHOOL

Bedwell Crescent,

Stevenage, Herts, SG1 1NJ

Updated September 2017

1 - Introduction

At Bedwell, we understand the responsibility to educate our pupils on eSafety 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.

Whilst exciting and beneficial both in and out of the context of education, much ICT, 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 Internet technologies and that some have minimum age requirements, usually 13 years. The nature and use of these resources is constantly changing, and currently includes:

- Websites
- Email, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting and video broadcasting

As a School, we also hold a huge amount of personal data on learners, staff and families. 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 also potentially damage the reputation of the school.

Everybody in the school 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 Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, 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).

2 – Acceptable Useage

All users are required to agree to the School's Acceptable Useage policies at the beginning of each academic year. Pupils are introduced to the agreement in assemblies and its key themes are reinforced by class teachers in Computing sessions. Copies are sent home and must be signed by both pupils and parents/carers before children are allowed to access ICT resources (see Appendices A and B).

Staff, governors and visitors must also sign-up to the School's Acceptable Useage Policy (see Appendix C), confirming that they will comply with this policy, take all practical measures to protect personal data and ensure that their use of ICT is compatible with their professional role at all times.

3 – Monitoring

Authorised staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact the School Office or Headteacher. Any authorised staff member will be happy to comply with this request.

Authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving employees or contractors, without consent, to the extent permitted by law. 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 1998, or to prevent or detect crime. Authorised staff may also, without prior notice, access the email or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000. Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual. Any policy breach is also grounds for further disciplinary action in accordance with the School Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated. Policy breaches may also lead to criminal or civil proceedings.

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

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT **must be immediately reported to the school's eSafety Co-ordinator, David Roberts**. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the eSafety Co-ordinator.

4 – eSafety

Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is David Roberts who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as HCC, Herts for Learning, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and governors are updated by the eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHCE

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school has a framework for teaching internet skills in Computing lessons, as part of the Computing Scheme of Work. eSafety is taught in every year group.
- eSafety is also covered in other curriculum areas, particularly PSHCE. Whenever the internet is to be used as a research tool (eg. in humanities or science lessons), key safe-searching points will be recapped.

- eSafety, particularly relating to cyberbullying and the use of social networks outside of school is also used as a regular assembly theme.
- Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; eg. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or the CEOP report abuse button.
- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.

eSafety Skills Development for Staff

- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

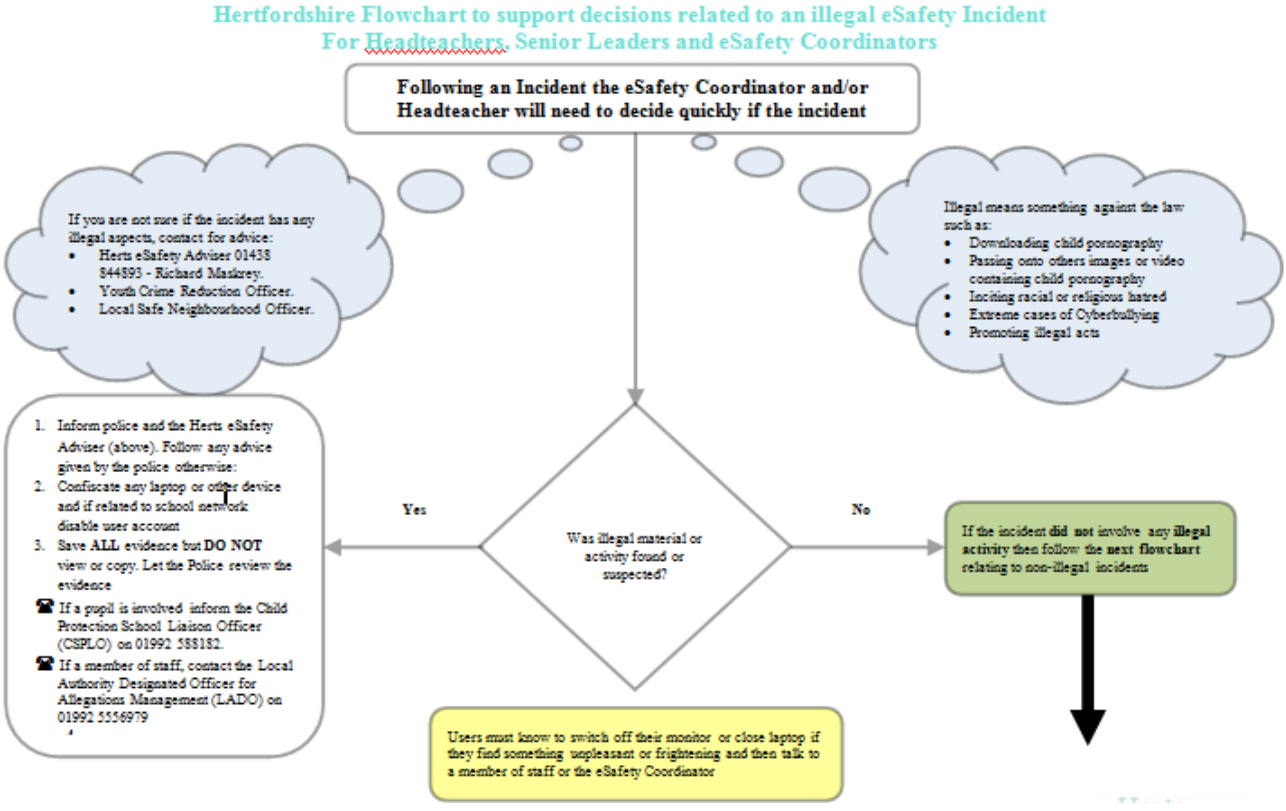
Managing the School eSafety Message

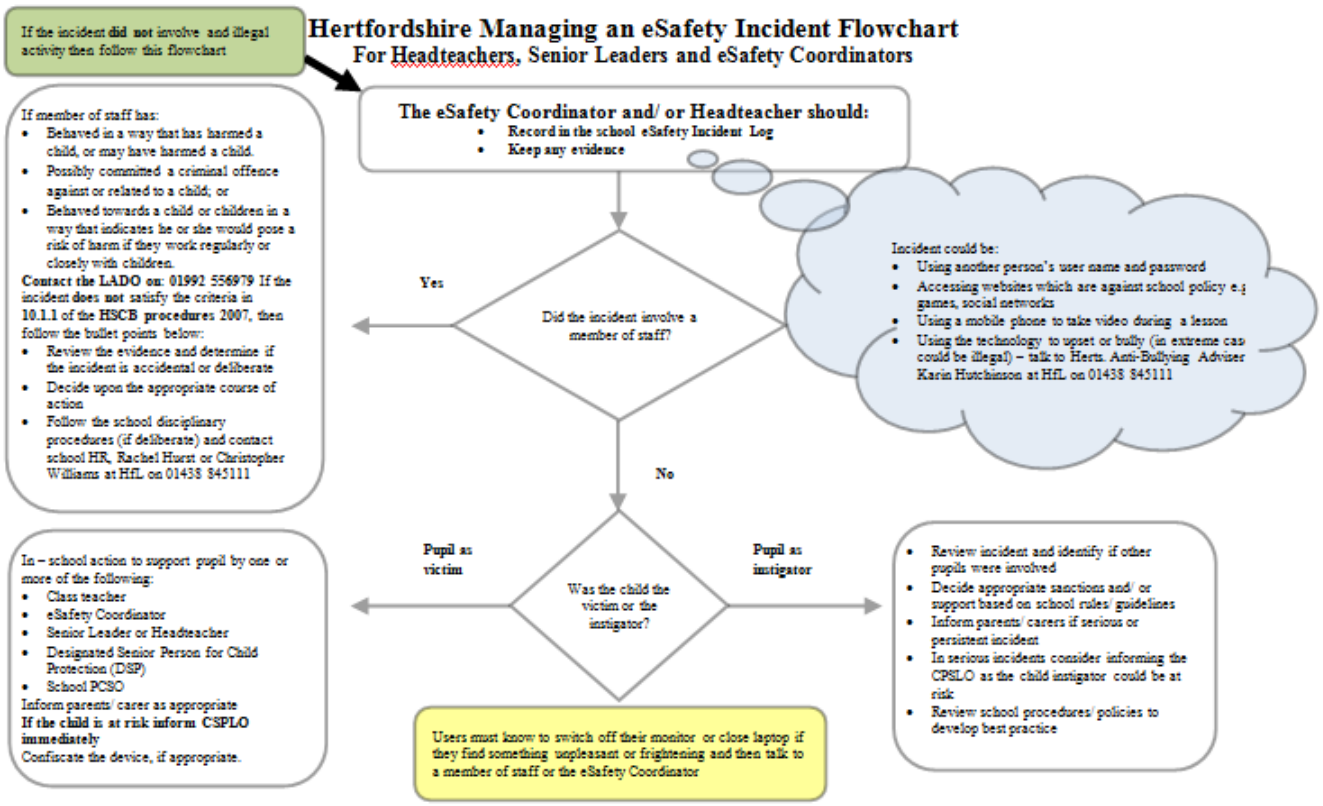
- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.
- The eSafety policy will be introduced to the pupils at the start of each school year.
- eSafety posters will be prominently displayed.
- The key eSafety advice will be promoted widely through school displays, newsletters, class activities and so on.
- We will participate in Safer Internet Day every February.

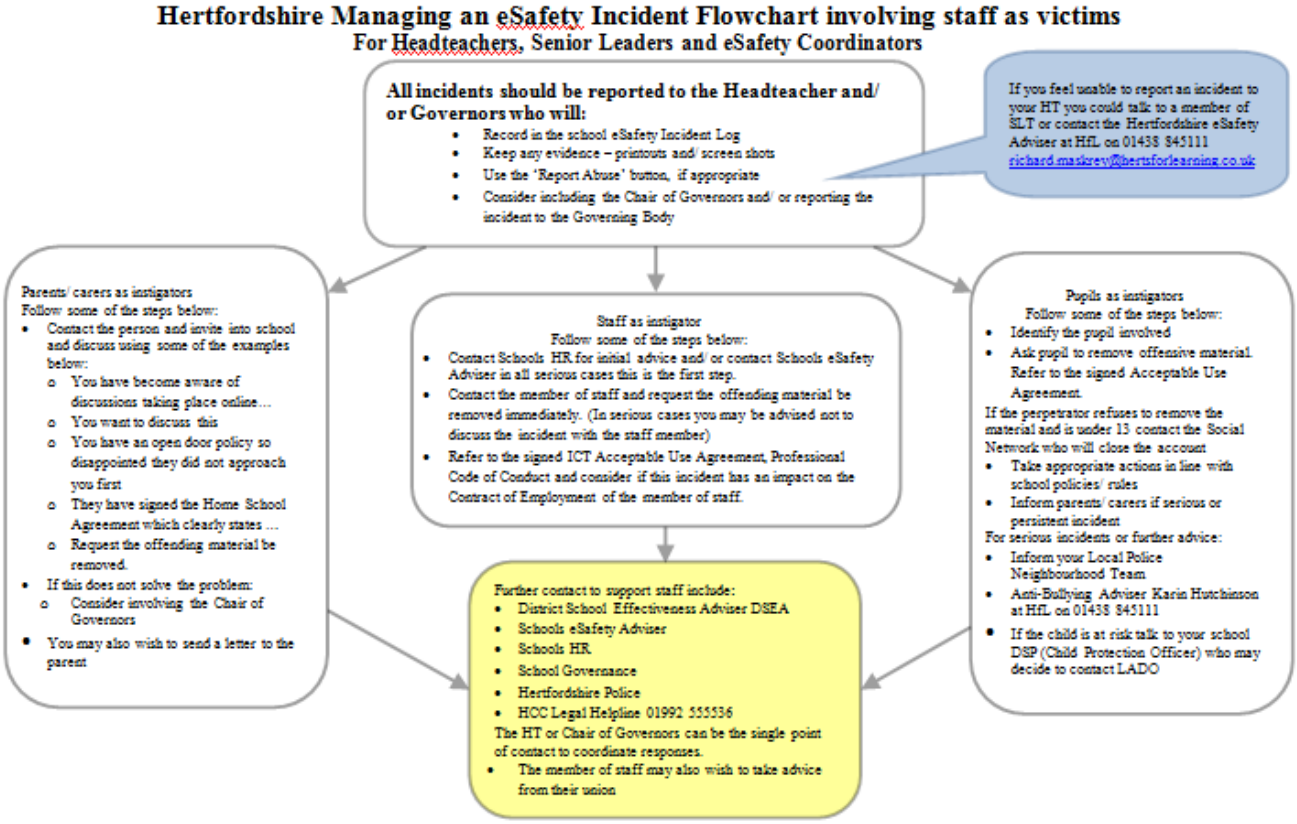
5 – Incident Reporting

Logging of incidents

- All eSafety incidents are logged by the eSafety Co-ordinator using the form in Appendix D.
- Any security breaches or attempts, loss or equipment and any unauthorised use of suspected misuse of ICT must be immediately reported to the school's relevant responsible person or eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), misuse or unauthorised use of ICT should be reported.
- Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Headteacher. Incidents should be logged and the Hertfordshire Flowcharts for Managing an eSafety Incident should be followed (see below).
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator and, depending on the seriousness of the offence, investigation by the Headteacher. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.




If the incident did not involve and illegal activity then follow this flowchart
Hertfordshire Managing an eSafety Incident Flowchart
For Headteachers, Senior Leaders and eSafety Coordinators
The eSafety Coordinator and/ or Headteacher should:
Record in the school eSafety Incident Log
Keep any evidence
If member of staff has:
Behaved in a way that has harmed a child, or may have harmed a child.
Possibly committed a criminal offence against or related to a child; or
Behaved towards a child or children in a way that indicates he or she would pose a risk of harm if they work regularly or closely with children.
Contact the LADO on: 01992 556979 If the incident does not satisfy the criteria in 10.1.1 of the HSCB procedures 2007, then follow the bullet points below:
Review the evidence and determine if the incident is accidental or deliberate
Decide upon the appropriate course of action
Follow the school disciplinary procedures (if deliberate) and contact school HR, Rachel Hurst or Christopher Williams at HfL on 01438 845111
Yes
Did the incident involve a member of staff?
Incident could be:
Using another person's user name and password
Accessing websites which are against school policy e.g games, social networks
Using a mobile phone to take video during a lesson
Using the technology to upset or bully (in extreme cas could be illegal) – talk to Herts. Anti-Bullying Adviser Karin Hutchinson at HfL on 01438 845111
No
Pupil as victim
Was the child the victim or the instigator?
Pupil as instigator
In – school action to support pupil by one or more of the following:
Class teacher
eSafety Coordinator
Senior Leader or Headteacher
Designated Senior Person for Child Protection (DSP)
School PCSO
Inform parents/ carer as appropriate
If the child is at risk inform CSPLO immediately
Confiscate the device, if appropriate.
Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to a member of staff or the eSafety Coordinator
Review incident and identify if other pupils were involved
Decide appropriate sanctions and/ or support based on school rules/ guidelines
Inform parents/ carers if serious or persistent incident
In serious incidents consider informing the CPSLO as the child instigator could be at risk
Review school procedures/ policies to develop best practice


Hertfordshire Managing an eSafety Incident Flowchart involving staff as victims
For Headteachers, Senior Leaders and eSafety Coordinators
All incidents should be reported to the Headteacher and/ or Governors who will:
Record in the school eSafety Incident Log
Keep any evidence – printouts and/ screen shots
Use the 'Report Abuse' button, if appropriate
Consider including the Chair of Governors and/ or reporting the incident to the Governing Body
If you feel unable to report an incident to your HT you could talk to a member of SLT or contact the Hertfordshire eSafety Adviser at HfL on 01438 845111
richard.maskrey@hertsforlearning.co.uk
Parents/ carers as instigators
Follow some of the steps below:
Contact the person and invite into school and discuss using some of the examples below:
You have become aware of discussions taking place online…
You want to discuss this
You have an open door policy so disappointed they did not approach you first
They have signed the Home School Agreement which clearly states …
Request the offending material be removed.
If this does not solve the problem:
Consider involving the Chair of Governors
You may also wish to send a letter to the parent
Staff as instigator
Follow some of the steps below:
Contact Schools HR for initial advice and/ or contact Schools eSafety Adviser in all serious cases this is the first step.
Contact the member of staff and request the offending material be removed immediately. (In serious cases you may be advised not to discuss the incident with the staff member)
Refer to the signed ICT Acceptable Use Agreement, Professional Code of Conduct and consider if this incident has an impact on the Contract of Employment of the member of staff.
Pupils as instigators
Follow some of the steps below:
Identify the pupil involved
Ask pupil to remove offensive material. Refer to the signed Acceptable Use Agreement.
If the perpetrator refuses to remove the material and is under 13 contact the Social Network who will close the account
Take appropriate actions in line with school policies/ rules
Inform parents/ carers if serious or persistent incident
For serious incidents or further advice:
Inform your Local Police Neighbourhood Team
Anti-Bullying Adviser Karin Hutchinson at HfL on 01438 845111
If the child is at risk talk to your school DSP (Child Protection Officer) who may decide to contact LADO
Further contact to support staff include:
District School Effectiveness Adviser DSEA
Schools eSafety Adviser
Schools HR
School Governance
Hertfordshire Police
HCC Legal Helpline 01992 555536
The HT or Chair of Governors can be the single point of contact to coordinate responses.
The member of staff may also wish to take advice from their union

6 – Parental Involvement

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

Engaging parents and carers

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school (see Appendix A).
- 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 (eg. on the school website).
- Parents / carers are provided with the knowledge, information and training required to manage their child's internet use, including setting privacy levels, understanding the potential dangers of social media and online interaction and the reasons why the 13+ ratings of services such as Facebook and Instagram should not be ignored.
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
  - Information and training sessions
  - Posters and leaflets
  - Information provided through newsletters and the School website

7 – Internet Access

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. All internet use through the

HICS network (Hertfordshire Internet Connectivity Service) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- The school provides pupils with supervised access to Internet resources through the school's fixed and mobile internet connectivity.
- Staff will preview any recommended sites, online services, software and apps before use.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- Users must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.
- Do not reveal names of colleagues, pupuls, others or any other confidential information acquired through your job on any social networking site or other online application.
- School internet access is controlled through the HICS web filtering service. For information on filtering see www.thegrid.org.uk/eservices/safety/filtered.shtml.
- The School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate.
- It is the responsibility of the school, delegated to the Network Technician, to ensure that anti-virus protection is installed and kept up-to-date on all machines.
- It is at the Headteacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.
- If there are any issues related to viruses or anti-virus software, the Computing Co-ordinator should be informed.

8 - Email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email 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 email in relation to their age and how to behave responsibly online.

Staff and governors should use a school email account for all official communication to ensure that children are protected through the traceability of all emails through the school email system. In addition, it is important that governors are protected against possible allegations of inappropriate contact with children. This is to help mitigate the chance of issues occurring and is an essential element of the safeguarding agenda.

Managing email

- The school gives all staff 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
- Staff and governors should use their school email address for all professional communication
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- Emails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.
- Pupils are introduced to email as part of the Computing Scheme of Work, and are taught how to use it safely and effectively, particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission.

- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting email

Emailing Personal or Confidential Information

Where your conclusion is that email must be used to transmit such data, use one of the following systems:

- Use Schoolsfx, Hertsfx or Hertfordshire's web-based Secure File Exchange portal that enables schools to send and receive confidential files securely
- Obtain express consent from your manager to provide the information by email. Verify the details of the intended recipient, encrypt and password protect attachments, send the encryption key in a separate email, and request confirmation of safe receipt.

9 – Social Media

Online technologies, including social networking sites, if used responsibly both outside and within an educational context 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. 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.

Pupils

- At present, the school endeavours to deny access to social networking and online games websites to pupils within 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 taught to avoid placing images of themselves (or details within images that could give background details) on websites and to consider the appropriateness of any images they post.
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are.

- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online.
- Our pupils are asked to report any incidents of Cyberbullying to the school.

Staff

- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using systems approved by the Headteacher.
- When signing up to online services that require the uploading of what could be deemed as personal or sensitive data, schools should check terms and conditions regarding the location of storage. Please see the Safe Harbour Agreement Statement www.thegrid.org.uk/info/dataprotection/#data and ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/10/ico-response-to-ecj-ruling-on-personal-data-to-us-safe-harbor/
- Services such as Facebook and Instragram have a 13+ age rating which should not be ignored.
- Our school uses Twitter to communicate with parents and carers. The Computing Coordinator is responsible for all postings and monitors responses from others.
- Staff are not permitted to access their personal social media accounts using school equipment at any time.
- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever

10 – Password Security

Staff Passwords

- Always use your own personal passwords. Passwords must contain a minimum of six characters, including a mixture of upper and lowercase letters, numbers and symbols and be difficult to guess.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Staff should change temporary passwords at first logon.
- Change passwords whenever there is any indication of possible system or password compromise.
- Do not record passwords or encryption keys on paper or in an unprotected file.
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
- Never tell a child or colleague your password.
- If you aware of a breach of security with your password or account inform the Computing Co-ordinator immediately.
- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's eSafety Policy and Data Security (see Appendix C).
- Pupils are not permitted to deliberately access online materials or files on the school network or local storage decides of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network and MIS systems, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

11 – Data Security

The accessing and appropriate use of school data is something that the school takes very seriously. HCC guidance documents can be found at:

www.thegrid.org.uk/info/dataprotection

Security

- The school gives relevant staff access to its Management Information System, with a unique username and password.
- It is the responsibility of everyone to keep passwords secure.
- Staff are aware of their responsibility when accessing school data.
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use (see Appendix C).
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data.
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight.
- It is the responsibility of individual staff to ensure the security of any personal or confidential information contained in documents copied, scanned or printed.

Relevant Responsible Persons

Members of the School's Senior Management Team (SMT) should be familiar with inforamtion risks and the school's response. One member of SMT should have a lead role on managing information risk, with the following responsibilities:

- they lead on the information risk policy and risk assessment
- they advise school staff on appropriate use of school technology
- they act as an advocate for information risk management

The designated lead on information risk in this school is currently **David Roberts.**

Protecting Personal or Sensitive Information

All staff should:

- Ensure that any school information accessed from their own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended.

- Ensure they lock their screen before moving away from their computer during the normal working day to prevent unauthorised access.
- Ensure the accuracy of any personal or sensitive information disclosed or shared with others.
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.
- Only download personal data from systems if expressly authorised to do so by their manager.
- Ensure hard copies of data are securely stored and disposed of after use.

12 – Safe Use of Images

Taking of Images and Film

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. HCC guidance can be found at:

www.thegrid.org.uk/eservices/safety/policies.shtml#images

- 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.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff 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 Headteacher.
- Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication.
- 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 (in writing) to use their child's work/photos in the following ways:

- on the school website.
- in the school prospectus and other printed publications that the school may produce for promotional purposes.
- recorded/ transmitted on a video or webcam.
- on the school's learning platform or Virtual Learning Environment.
- in display material that may be used in the school's communal areas.
- in display material that may be used in external areas (eg. exhibitions promoting the school).
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

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, eg divorce of parents, custody issues, etc. Parents or carers may withdraw permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa. Email 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.

Only the Computing Co-ordinator has authority to upload to the school website.

For further information relating to issues associated with school websites and the safe use of images in Hertfordshire schools, see

www.thegrid.org.uk/schoolweb/safety/index.shtml
www.thegrid.org.uk/info/csf/policies/index.shtml#images

Storage of Images

- Images/ films of children are stored on the school's network.
- Pupils and staff are not permitted to use personal portable media for storage of images (eg. USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource
- The Computing Co-ordinator has the responsibility of deleting the images when they are no longer required, or when the pupil has left the school.

13 – Safe Use of ICT Equipment

School ICT Equipment

- All users of school ICT equipment are responsible for their activity.
- Visitors should not be allowed to plug hardware into school network points (unless special provision has been made).
- All ICT equipment must be kept physically secure.
- It is imperative that all users save their data on a frequent basis to the school's network. Users are responsible for the backup and restoration of any of their data that is not held on the school's network.
- Personal or sensitive data should not be stored on the local drives of desktop PCs, laptops, USB memory sticks or other portable device. If it is necessary to do so the local drive must be encrypted.
- A time locking screensaver should be applied to all machines. Any device accessing personal data must have a locking screensaver.
- It is the responsibility of all users to ensure that any information they access is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.
- Personal equipment may only be used with consent of the Headteacher.

Disposal of Redundant ICT Equipment

- 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 overwritten multiple times to ensure that data is irretrievably destroyed. If storage media has failed, it will be physically destroyed. We 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 (WEEE) Regulations 2006
  - the Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
  - Data Protection Act 1998
  - Electricity at Work Regulations 1989

- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

Servers

- The School server is only to be accessed by the Computing Co-ordinator and Network Technician. No other staff should attempt to logon to this machine.
- The Server should never be left logged-on when unattended (even for very brief spaces of time).
- Data must be backed up regularly (at least weekly; preferably daily). Back-up tapes should be encrypted by appropriate software and should be securely stored in a fireproof container.
- Remote back-up of MIS data should be automatically securely encrypted.

Systems & Access

Key messages for all users:

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC.
- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you.
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access.
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time.
- Do not introduce or propagate viruses.
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or HCC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations

Act and the Disability Discrimination Act).

- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act.
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998
- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a written guarantee that they will irretrievably destroy the data by multiple over writing the data.

14 – Reviewing this Policy

Staff and pupil involvement in policy creation

Staff, governors and pupils have been involved in making/ reviewing the eSafety policy through discussions at staff meetings, SMT and School Council.

Review Procedure

There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety that concerns them.

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

This policy will be reviewed every twelve months and consideration given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

This policy has been read, amended and approved by the staff, head teacher and governors during September 2017.

Appendix A – Pupils Acceptable Use Agreement

Bedwell School
Pupil Acceptable Use of ICT Agreement

- ✓ I will only use ICT in school for school purposes.
- ✓ I will not tell other people my ICT passwords.
- ✓ I will only open/delete my own files.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ When learning about email, I will only use my class email address or a school email address given to me by my teacher.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not give out my own details such as my 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 and a responsible adult comes with me.
- ✓ I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community.
- ✓ I will not use any online service at school unless this is an agreed part of a school project, approved by my teacher.
- ✓ I will not sign-up to online services like Facebook and Instagram until I am old enough.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

Pupil Signature : …….. Class : ……

Parent/ Carer Signature …… Date : ……..

Appendix B – Letter to Parents

Dear Parent/ Carer

ICT is an important part of learning in our school, giving our children the chance to quickly gather information from around the world, communicate with other people and share their thoughts and feelings in a huge number of ways. However, as well as these fantastic advantages, ICT (and the internet in particular) can also present new hazards if it is not used safely.

In assembly today, we have discussed our school rules for eSafety, which all children need to sign-up to. Please could you read and discuss the attached copy with your child, and return them with both of your signatures as soon as possible.

We also talked about how safely we are using computers at home (particularly to access sites like YouTube and Facebook which are blocked at school), so this might also be a good opportunity to discuss the way your children use the internet at home, and think about who they are communicating with and what information they are sharing online. I have attached a parents' guide produced by Childnet which includes both ideas for starting those conversations and the 5 'SMART' rules for safe internet usage that we follow at School - and there is lots more useful information on their website (www.childnet.com) and the ThinkUKnow site (thinkuknow.co.uk).

If you have any concerns or would like further explanation of any of this, please contact your child's teacher.

Many thanks for all your support,

Mr D Roberts
Computing Co-ordinator & Assistant Head

Appendix C – Staff, Visitors & Governors Agreement

Staff, Governor and Visitor Acceptable Use of ICT Agreement & Code of Conduct

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

- I will only use the school's email / Internet / Intranet / Learning Platform and related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account or any other social media link, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher.
- I will not install any hardware of software without permission of the Computing Co-ordinator.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I will support the School apprach to online safety and not upload or add any images, video, sounds or text linked to or assoociated with the school or its community.
- 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 Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.
- I will support and promote the school's eSafety and Data Security policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand that this forms part of the terms and conditions set out in my contract of employment.

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)

Appendix D – Incident Log

Details of ALL eSafety incidents are to be recorded by the eSafety Co-ordinator. This incident log will be monitored termly by the Headteacher, Members of SMT or Chair of Governors. Any incidents involving cyberbullying may also need to be recorded elsewhere.

Date & Time	Name of pupil or staff member	Computer number / location	Details of incident	Actions & reasons

Appendix E – Current Legislation

Acts Relating to Monitoring of Staff email

Data Protection Act 1998
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 individuals rights of access to their personal data, compensation and prevention of processing. **www.hmso.gov.uk/acts/acts1998/19980029.htm**

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 **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. **www.hmso.gov.uk/acts/acts2000/20000023.htm**

Human Rights Act 1998
www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to eSafety

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 so to fear on each of those occasions.

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.

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 a 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.

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.

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 persons 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.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (email) 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.

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.

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 them 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.

Racial and Religious Hatred Act 2006
It 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.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article (including electronic transmission) is a criminal offence.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998
www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 2000
https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

Counter-Terrorism and Security Act 2015 (Prevent)

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