BOLD FUTURES

E-Safety Policy

Next Review : Feb 2026

Signed by:

_____ Headteacher Date: _____

_____ Chair of governors Date: _____

Last updated: 7th February 2025

E-safety Policy

POLICY CHANGE HISTORY

Version	Date	Status	Policy Owner	Governor Approval	Comment
1.0	November 2021		L.Coombs		
2.0	November 2023		L.Coombs		Update of roles and responsibilities Additional information added about filtering and monitoring Flow chart added to explain process of misconduct
2.1	October 2024		L.Coombs		No changes required
2.2	October 2025		L.Coombs		Update to be across federation document

E-safety Policy

This Online Safety Policy outlines the commitment of the Bold Futures Federation to safeguard members of our federation community online in accordance with statutory guidance and best practice. It has been written in accordance with current government guidance and agreed by the Designated Safeguarding Leads and Governors.

This Online Safety Policy applies to all members of the federation community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of each school's digital systems, both in and out of the school sites. It also applies to the use of personal digital technology on each school site (where allowed).

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

Rationale

As a federation of schools, we are confident that internet use enhances educational opportunities, professional development, data management and administration. However, at all times the safety and well-being of our children is the primary concern. This policy applies to the federation governing body, all teaching and other staff, whether employed by the County Council or employed directly by the federation, external contractors providing services on behalf of the federation or the County Council, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the federation. These individuals are collectively referred to in this policy as staff or staff members. This policy should be read in conjunction with the federation's Safeguarding, Whistleblowing, Child Protection, Data Protection, Anti-bullying and Social Media policies and staff acceptable use of ICT policy.

The internet is seen as an integral part of modern-day life and is an essential resource in supporting teaching and learning as well as being part of the statutory curriculum. The use of the internet and other digital technologies in school and at home help to stimulate learning, promote discussion and increase awareness of the wider world helping to raise educational standards and promote student achievement. Across the federation, we aim to provide children with learning opportunities and experiences which build ICT skills needed to access life-long learning and employment in this rapidly changing world; improving their understanding of doing so in a safe and responsible manner. Through our curriculum we aim to help children begin to be able to evaluate Internet information and begin to take care of their own safety and security both in school and at home.

However, we also understand the use of these new technologies can put young people at risk both within and outside the school setting. The DfE Keeping Children Safe in Education guidance suggests that the breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- ***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.*

As with all other risks, it is impossible to eliminate these completely. It is therefore essential, through good learning opportunities, to build pupils' resilience to the risks that they may experience, so that they have the confidence and skills to face and deal with them. The Bold Futures federation must demonstrate that it has provided the necessary safeguarding to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks.

Use of Internet in school

There are many reasons why as an educational setting we choose to use the internet.

- Internet Allows for the teaching of the Computing National Curriculum.
- Access to world-wide educational resources including images and videos.
- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to national developments and online training courses.
- Access to educational materials and effective curriculum practice.
- Collaboration across support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Exchange of curriculum and administration data such as WONDE.
- Access to learning wherever and whenever convenient.
- To promote and celebrate the achievements of the school through a website.
- Video calls to access training, professional development or meetings with other professional services.

Responsibilities

To ensure the online safeguarding of members of our federation community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within each school.

Headteacher and senior leaders

- The Collaboration Headteacher and Head of Schools have a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding. However, the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher and Strategic Senior Leadership team will be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead, Online Safety Lead, IT provider and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from the Computing Lead.
- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL), Computing lead and IT service providers in all aspects of filtering and monitoring.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy
This review will be carried out by the Governor for Safeguarding, a role which includes Online Safety, who will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Safeguarding Governor to include:

- **regular meetings with the Designated Safeguarding Lead / Computing Lead**
- **regularly receiving (collated and anonymised) reports of online safety incidents**
- **checking that provision outlined in the E-safety and Computing and ICT Policy**
- **Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually.** (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor)
- **reporting to relevant *governors***
- Receiving (at least) basic cyber-security training

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Designated Safety Leads (DSLs)

The DSL (with support from the Computing Lead will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the Safeguarding governor (alongside the Computing Lead) to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings
- report regularly to headteacher/senior leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Computing (Online Safety) Leads

The Online Safety Lead will:

- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL),
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- ensure that the online safety curriculum is planned, mapped, embedded and evaluated through:
    - a discrete programme
    - A mapped cross-curricular programme
    - assemblies and pastoral programmes
    - through relevant national initiatives and opportunities e.g. Safer Internet Day
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
    - content
    - contact
    - conduct
    - commerce

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to a DSL on the Computing Lead) for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers are on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*

- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

IT Provider

If the school has a technology service provided by an outside contractor, it is the responsibility of the school to ensure that the provider carries out all the online safety measures that the school's obligations and responsibilities require. It is also important that the provider follows and implements school Online Safety Policy and procedures.

The IT Providers (Agile/ HARRAP) and Internet provider (Schools Broadband/ HARRAP) are responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the Computing Lead/ DSL for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- monitoring systems are implemented and regularly updated as agreed in school policies

Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers

The school will take every opportunity to help parents and carers understand online safety issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement

- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc
- engaging parents/ carers in their role in supporting their child/ children online through parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school.
- the safe and responsible use of their children's personal devices in the school (where this is allowed)

School Website Content

- The contact details on each school website should be the school address, e-mail and telephone number. Staff or pupil's personal information must not be published.
- Only the school office e-mail should be available on the site.
- Whilst the Senior Leadership Team, the ICT lead and administration staff may edit and add to the school website, The Head teacher will have final approval about website content to ensure it is accurate and appropriate.
- The website will comply with the DfE guidelines for publications including respect for intellectual property rights and copyright.
- Pupil's full names will not be used anywhere on the website.
- Written permission from parents or carers will be obtained before images or videos of pupils are electronically published.
- The copyright of all material must be held by the school, or no copyright must be needed. Where permission to reproduce has been obtained, content must be attributed to the owner.

Social Networking

This policy should be read in conjunction with the 'Social Media Policy', where detailed information on social networking is given. Here is some further information for reference:

- Social Networking sites (eg. Facebook, Bebo, MySpace etc) are blocked or filtered on school computers as far as possible.
- Video websites such as Youtube are not blocked on our school computers as it is used by staff as a teaching aid. Pupils will not have access to video websites such as Youtube themselves at school.
- Pupils will be taught never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, phone numbers, school attended, full names of friends, specific interests and clubs etc.
- Parents will be advised that pupils across the federation are too young to have social network accounts and that they should not have access to other people's accounts either.
- Advice should be given regarding details in photographs which are uploaded to social media which could identify a pupil or staff member or his/her location eg. House number, street name or school.
- Parents will be told that any images of their own child on social media must not include the faces of, or information about, any other pupils or staff unless they have the permission of that pupil's parents or the staff member.

- Staff will be advised that they should keep any contact with parents on a professional basis and should not use social networking to contact parents.
- Regular updates regarding social media changes will be provided to parents through our school newsletters and during parent assemblies.
- Staff may have personal social networking accounts, but should be mindful of the content they write, share or upload and understand the privacy settings of their accounts to ensure they do not damage the reputation of themselves or the school. See more in section 13 'School Reputation and Confidentiality', and the section titled 'Cyber Bullying and Harassment of/by Staff and Other Adults'.

Video Conferencing

Video conferencing is a useful tool for staff to communicate with each other and to remotely teach pupils when necessary. When video conferencing with staff or pupils, the following guidelines will be adhered to:

- All videos being shared with pupils will be pre-recorded and watched by a staff member before being shown to pupils, to ensure they are suitable.
- All content being shared with pupils will only be shared with pupils of the appropriate age and maturity. Parental consent will be gained before showing pupils anything rated 'PG' (parental guidance).
- The copyright of all material being shared in video conferencing must be held by the school, or no copyright must be needed. Where permission to reproduce has been obtained, content must be attributed to the owner.
- Staff will be mindful of what can be seen and heard in the background when video conferencing, to make sure images and sounds are appropriate, non-offensive and do not breach individual privacy (eg. full names or addresses on display, images of other people, potentially offensive images etc).
- Staff generally should not share confidential or private information about themselves or others via video conferences. However, if such sharing is required staff will ensure the video conference is password protected and if the conference is saved, it is encrypted to keep private information safe.
- If a video conference is going to be recorded to be viewed again later, all people in the video conference will be informed before recording begins so that proper consent can be given.
- When screen-sharing during video conferencing, ensure that any documents being used on the computer of a confidential nature are not shown, or are closed prior to beginning screensharing.
- Video conferencing between staff will be accessed using accounts created with staff email addresses (predominately through Google Meet). All Child Protection, Safeguarding, Whistleblowing and Social Media Policies apply when working remotely using video conferencing.

Portable Devices

'Portable devices' includes, but is not limited to, mobile phones, tablets, games consoles, laptop computers, personal organisers, smart watches and internet connected toys. Many of these devices, particularly tablets and laptop computers, have a multitude of different and useful functions and it can be educational to use them in school. Teachers will be able to evaluate their use for a particular function.

- Portable devices will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- Staff mobile phones will generally not be used during lessons or formal school time to make or receive calls/messages.
- Pupils are not permitted to bring their personal portable devices into school (if this becomes a necessity, these will be stored safely in the school office).
- Parents will be reminded that any images taken using portable devices on school property must not include any information which would jeopardise the confidentiality and safety of others (such as pictures including other people's faces, full names or location). Images or recordings of other people may not be taken without their permission.
- All people using portable devices to make phone calls, video calls or to capture photographs and videos will be reminded to be mindful of the background images and sounds, and that others can easily hear what they are saying.
- Games consoles typically will not be used in school. Pupils are not permitted to bring their games consoles into school.

Assessing the Risk

Each school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer.

- There are filters in place to ensure content is suitable for children at an age-appropriate level
- The ICT leads will run regular safeguarding reports on internet usage of both pupils within their school and staff both within school and when using the school remote server. Results from these reports will be kept securely on file.
- Each school will periodically audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

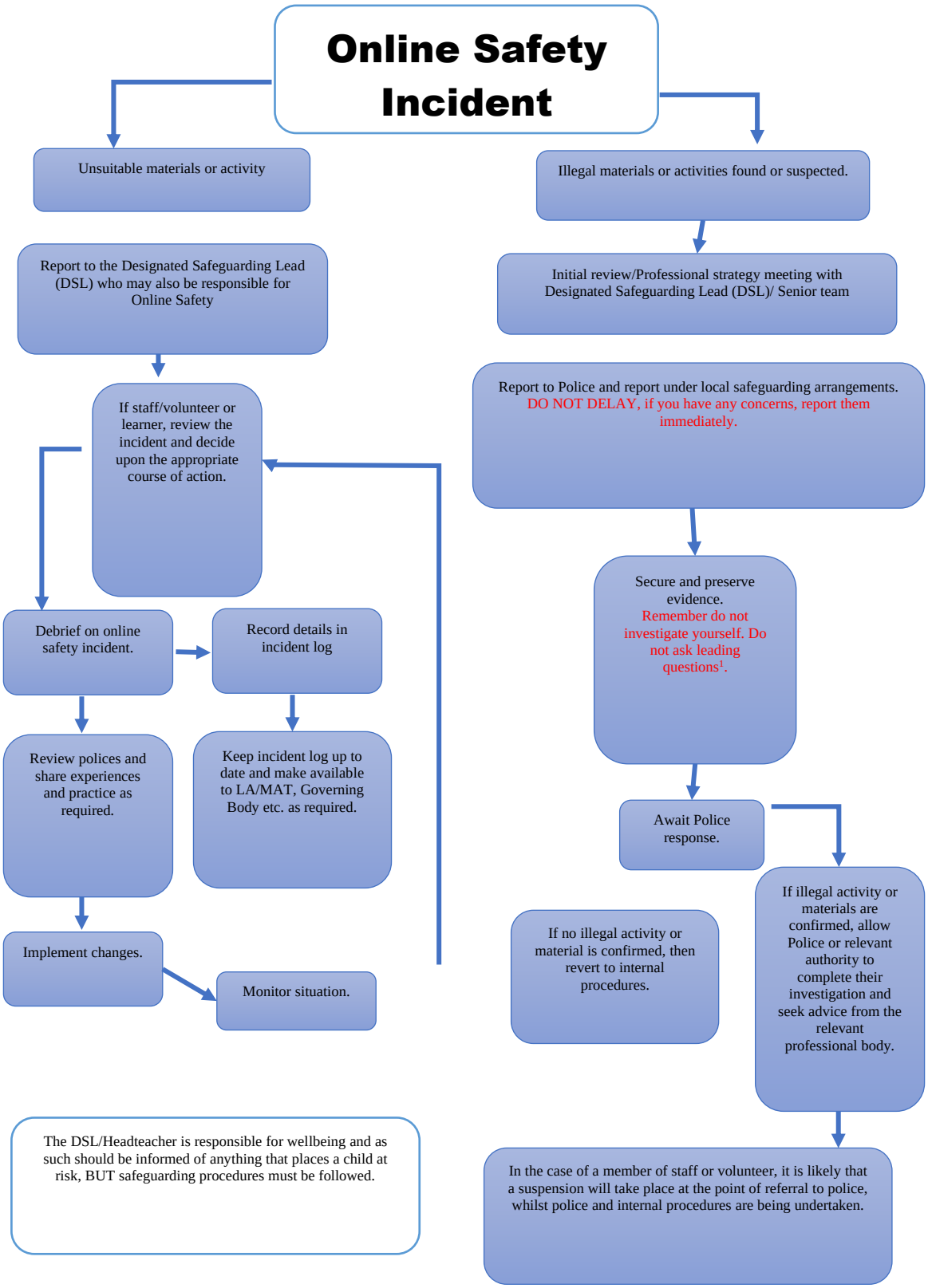
Procedures when Concerns are raised

Each school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The Federation will ensure:

- **there are clear reporting routes which are understood and followed by all members of each school community which are consistent with the federation safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.**
- **all members of the federation community will be made aware of the need to report online safety issues/incidents**
- **reports will be dealt with as soon as is practically possible once they are received**
- **the Designated Safeguarding Lead, Computing Lead and other responsible staff have appropriate skills and training to deal with online safety risks.**
- **if there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through the agreed federation safeguarding procedures. This may include**
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming

        - Extreme Pornography
        - Sale of illegal materials/substances
        - Cyber or hacking
        - Copyright theft or piracy
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Executive Headteacher or Head of Schools, in which case the complaint is referred to the Chair of Governors
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
    - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
        - internal response or discipline procedures
        - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- learning from the incident (or pattern of incidents) will be provided anonymously to:
    - *staff, through regular briefings*
    - *learners, through assemblies/lessons*
    - *parents/carers, through newsletters, school social media, website*
    - *governors, through regular safeguarding updates*

Each school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.



Inappropriate handing of school IT equipment by pupils will be dealt with in accordance to our federation Behaviour Policy.

Federation reputation and confidentiality

The federation recognises an employee's right to a private life. However, the federation must also ensure its reputation and confidentiality are protected. Therefore, an employee using any ICT away from school, including email and social networking sites must:

- Refrain from identifying themselves as working for the federation in a way that could have the effect of bringing the federation into disrepute.
- Not express a personal view as a federation employee that the federation would not want to be associated with.
- Notify a member of SLT immediately if they consider that content posted via any information and communications technology, including emails or social networking sites, conflicts with their role in the federation.
- Not have any unauthorised contact or accept 'friend' requests through social media with any pupil/student under the age of 18 (including former pupils) unless they are family members.
- Exercise caution when having contact or accepting 'friend' requests through social media with parents so as not to compromise the federation's reputation or federation information.
- Not allow interaction through information and communications technology, including emails or social networking sites, to damage relationships with work colleagues in the federation and/or partner organisations, pupils/students or parents.
- Not disclose any data or information about the federation, colleagues in the federation and/or partner organisations, pupils/students or parents that could breach the Data Protection Act 2018.
- Not use the Internet or social media in or outside of work to bully or harass other staff or others. See the section below titled 'Cyber Bullying and Harassment of/by Staff and Other Adults'.

External Use

Any use of school ICT equipment outside of school hours must comply with this policy. Digital equipment provided by the federaation which is being used by staff at home should be used for work purposes only.

Filtering & Monitoring

Each school's filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSLs (with support from the Computing Lead will have lead responsibility for safeguarding and online safety and the IT service provider (Schools Broadband/ HARRAP) will have technical responsibility.

The filtering and monitoring provision is reviewed termly by the Computing Lead, the Designated Safeguarding Lead and reported to a governor using a test filtering website (SWGfL Test Filtering)

Filtering

- the school manages access to content across its systems for all users and on all devices using the school's internet provision (Schools Broadband/ HARRAP).

- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- *each school has provided differentiated user-level filtering for staff and learners*
- *younger learners will be encouraged to use child friendly/age-appropriate search engines e.g. SWGfL Swiggle*
- *the school has a mobile phone policy and where personal mobile devices have no access to the school's internet*

If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Monitoring

Each school has monitoring systems in place to protect the school, systems and users:

- Each school monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

Each school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These may include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- *pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.*
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems
- use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)

Technical Security

Each school's technical systems will be managed in ways that ensure that the school meets recommended technical requirements

- responsibility for technical security resides with SLT who may delegate activities to identified roles.
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the SLT
- password policy and procedures are implemented.

- the security of their username and password must not allow other users to access the systems using their log on details.
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.
- the administrator passwords for all school systems are kept in a secure place, e.g. school safe.
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- Agile are responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider
- removable media is not permitted unless approved by the SLT/IT service provider
- guest users are provided with appropriate access to school systems based on an identified risk profile.

E-Safety (Online safety) Awareness at Bold Futures Federation

<u>Teaching of Online safety to pupils</u>

- Each year group will have a dedicated study on online safety (see below titled curriculum overview). This will provide an opportunity for children to extend their understanding of how to be a good online citizen and will provide a platform for discussions on how to stay safe online. This will be taught using age-appropriate material, such as CEOPs resources and Project Evolve (government produced resources).
- E-Safety assemblies will take place periodically to remind the children of safe and respectful internet use.
- Each year the federation will participate in the National Online Safety week which will provide children with up-to-date learning of key messages.

<u>Cyber Bullying, child-on child abuse and Harassment</u>

Cyber-bullying is defined as 'an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself.' By cyber-bullying, we mean:

- Bullying by electronic media.

- Bullying by texts or messages or phone calls.
- The use cameras to cause distress, fear or humiliation.
- Posting threatening, abusive, defamatory or humiliating material on websites, including blogs, personal websites, social networking sites
- Using e-mail to message upsetting content to others.
- Hijacking/cloning e-mail accounts.
- Making threatening, abusive, defamatory or humiliating remarks in on-line forums including during 'online chats' within gaming apps/ websites.

Cyber Bullying and Harassment of/by Pupils

The federation policy for correct procedures regarding a pupil being cyber-bullied is outlined in detail in the federation's Safeguarding policy which must be read by all staff.

Cyber Bullying and Harassment of/by Staff and Other Adults

This section should be read in conjunction with the Department of Education guidance contained in "Cyber-bullying: Advice for Headteachers and School Staff". The federation will consider it a potential disciplinary matter if staff utilise any information and communications technology, including email and social networking sites, in such a way as to bully or harass others in the federation, in professional organisations, pupils or parents, whether this takes place during or outside of work. Staff members need to be aware that no matter what the privacy settings on their social media site, inappropriate or derogatory information about a colleague, pupil or parents can find its way into the public domain even when not intended. It should be noted that a person does not need to directly experience this form of victimisation in order for it to be classed as cyber bullying/harassment. The fact that a person is unaware that offensive or derogatory comments about them have been placed on websites still fits the criteria of cyber bullying/harassment. If a staff member receives any threats, abuse or harassment from members of the public online then they must report such incidents to the Senior Leadership Team, or where necessary the police. Support is also available through Hampshire's confidential counselling service, Employee Support (0800 030 5182). The federation owes a duty to take reasonable steps to provide a safe working environment free from bullying and harassment. For this reason, it is essential that the Senior Leadership Team take appropriate steps to deal with any incident where it is alleged that a staff member has subjected others to abusive or personally offensive emails, phone calls or content on social networking sites such as Facebook, Twitter, Youtube or by any other means. If a Senior Leader is made aware of such an allegation, the Senior Leadership Team should deal with it in the same way as any other incident of bullying or harassment in line with federation policies, by investigating the allegations promptly and appropriately and providing the victim with support which demonstrates that the matter is being dealt with seriously. Senior Leaders should encourage staff to preserve all evidence by not deleting emails, logging phone calls and taking screen-prints of websites. If the incident involves illegal content or contains threats of a physical or sexual nature, the Senior Leadership team should consider advising the employee that they should inform the police. In the event that such evidence contains indecent images of children, it is an offence to save, send, or alter an image or to show it to anyone else. Therefore, the evidence must be placed in a secure location such as a locked cupboard where others will not be able to see it. In these circumstances the Police should be contacted immediately for advice.