AYLSHAM LEARNING FEDERATION

ONLINE SAFETY POLICY

Policy Reference:	JT//KHOnline Safety	Review Frequency:	1 Year
Issue Number:	07 (19.09.2023)	Next Review Date:	19.09.2024
Author:	J. Tuttle/K. Harris		

Ratified by the Governors' Curriculum Committee on: 19.09.2023

Signed: .....

Chair

This policy should be read in line with the Federation's statutory safeguarding including child protection policy. Any issues and concerns with online safety must follow the Federation's safeguarding and child protection processes. This policy applies to all members of Aylsham Learning Federation community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of Federation technologies, both in and out of Aylsham Learning Federation. It also applies to the use of personal digital technology on the school site (where allowed).

Contents

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the Federation community at Aylsham High School, Bure Valley School, John of Gaunt Infant and Nursery School and John Bear's Nursery with respect to the use of technologies.
- Safeguard and protect all members of the schools' community online in accordance with statutory guidance and best practice.
- Assist Federation staff working with children to work safely and responsibly with technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of technologies for educational, personal or recreational use for the whole Federation community.
- Have clear structures to deal with online abuse such as online bullying.
- Ensure that all members of the Federation community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.
- Establish clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms.

The Issues classified within online safety are considerable, but main areas of risk for our Federation community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content (fake news)

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Commerce

- Online gambling
- Financial scams
- Hidden costs and advertising in apps, games and website

How the policy is communicated to staff/pupils/community

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on each school's/setting's website/staffroom/relevant classroom.
- Policy to be part of each school's/setting's induction pack for new staff, including information and guidance where appropriate.
- All staff must read and sign the ICT acceptable use policy (staff/governors/visitors)' before using any school/setting technology resource.
- Regular updates and training on online safety for all staff, including any revisions to the policy.
- ICT acceptable use policy (staff/governors/visitors, and pupils) discussed with staff and pupils (if applicable) at the start of each year. ICT acceptable use policy (staff/governors/visitors) to be issued to members of each school's/setting's community, on entry to the school.

Handling Concerns

- The Federation will take all reasonable precautions to ensure online safety is in line with current guidance from the Department for Education (DfE).
- Staff and pupils are given information about infringements in use and possible sanctions.
- Designated Safeguarding Lead/(s) (DSL) act as first point of contact for any safeguarding incident whether involving technologies or not.
- Any concern about staff misuse is always referred directly to the Executive Headteacher/DSL (Aylsham High School only), or Headteacher unless the concern is about the Executive Headteacher in which case the concern is referred to the Chair of Governors and the local authority.

Review and Monitoring

The online safety policy should be referenced within other Federation policies (e.g. safeguarding and child protection policy, anti-bullying policy, PSHE).

- The online safety policy will be reviewed annually **or** when any significant changes occur with regard to the technologies in use within the Federation.
- The online safety group will assist with the development and review of the policy.
- There is widespread ownership of the policy and it has been agreed by the Senior Leadership Team/(s) (SLT) and approved by governors. All amendments to the Federation online safety policy will be disseminated to all members of staff and pupils.
- The Federation schools will monitor the impact of the policy using; logs of reported incidents, and monitoring logs of internet activity.

2. Policy and Leadership

Headteacher and senior leaders

- The Executive Headteacher/Headteacher has a duty of care to ensure the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the DSL and online safety lead.
- The Executive Headteacher/Headteacher and (at least) another member of the senior leadership team should 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 Executive Headteacher/Headteacher/SLT are responsible for ensuring that the online safety lead, technical staff, 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 Executive Headteacher/Headteacher/SLT 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 Executive Headteacher/Headteacher/SLT will receive regular monitoring reports from the online safety lead.

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body".

This review will be carried out by the curriculum committee whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing board will take on the role of online safety governor to include:

- regular meetings with the online safety lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the online safety policy (e.g. online safety education provision and staff training is taking place as intended)
- reporting to relevant governors group/meeting
- membership of the school online safety group (attendance as and when requested)
- occasional review of the filtering change control logs and the monitoring of filtering logs (where possible)

The Governing Board will also support the Federation in encouraging parents/carers and the wider community to become engaged in online safety activities.

Online Safety Lead

Schools within the federation will have a named member of staff with a day-to-day responsibility for online safety; in some schools this will be combined with the DSL role.

The online safety lead will:

- lead the online safety group (on rotation)
- work closely on a day-to-day basis with the DSL/(s)
- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- have a leading role in establishing and reviewing the Federation online safety policies/documents
- promote an awareness of and commitment to online safety education/awareness

raising across the schools and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- 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
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- provide (or identify sources of) training and advice for staff/governors/parents/ carers/learners
- liaise with (school/local authority/external provider) technical staff, pastoral staff and support staff (as relevant)
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- attend relevant governing board meetings/groups
- report regularly to Executive Headteacher/Headteacher/SLT.

Designated Safeguarding Lead/s (DSL)

- Kathryn Garnham – Aylsham High School
- Jamie Olney – Bure Valley School
- ClareToplis – John of Gaunt Infant and Nursery and
- Clare Toplis - John Bears Nursery

are the designated Federation safeguarding leads responsible for safeguarding and child protection (including online safety).

Technology provides additional means for safeguarding issues to develop. Where the roles of the DSL and the online safety lead are not combined, they will work closely in collaboration due to the safeguarding issues often related to online safety.

The DSL is trained in online safety issues and aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying

Curriculum Leads
Curriculum leads will work with the online safety lead to develop a planned and coordinated online safety education programme e.g. ProjectEVOLVE.

This will be provided through:
- a discrete programme;
- PSHE and SRE programmes;
- A mapped cross-curricular programme;
- assemblies and pastoral programmes;
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and support staff

Federation staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current Federation's 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 the safeguarding team for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers should be on a professional level and only carried out using official Federation 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 should be 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, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGFL Safe Remote Learning Resource
- have 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.

Network manager/technical staff

The network manager/technical staff (or local authority/technology provider) is responsible for ensuring that:

- they are aware of and follow the Federation's online safety policy to carry out their work effectively in line with Federation policy
- the Federation technical infrastructure is secure and is not open to misuse or malicious attack
- the Federation meets (as a minimum) the required online safety technical requirements as identified by the local authority or other relevant body
- 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 online safety lead 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 (see appendix 'Technical Security Policy template' for good practice).
- monitoring software/systems are implemented and regularly updated as agreed in Federation policies

Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and online safety policy (this should include personal devices – where allowed)
- 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 Federation's online safety policy covers their actions out of school, if related to their membership of the school.

The Federation acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. It recognises the potential for this to shape the online safety strategy for the Federation community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- mechanisms to canvas learner feedback and opinion.
- appointment of digital leaders/friendly faces/peer mentors
- the online safety group has learner representation
- learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns
- learners designing/updating acceptable use agreements
- contributing to online safety events with the wider Federation community e.g. parents' evenings, family learning programmes etc.

Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The Federation will take every opportunity to help parents and carers understand these issues through:

- publishing the Federation online safety policy on the school website
- providing them with a copy of the learners' acceptable use agreement (the school will need to decide if they wish parents/carers to acknowledge these by signature)
- publish information about appropriate use of social media relating to posts concerning the school and or Federation
- seeking their permissions concerning digital images, cloud services etc (see parent/carer AUA in the appendix)
- 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 Federation in:

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

Online Safety Group

The online safety group provides a consultative group that has wide representation from the Federation community, with responsibility for issues regarding online safety and monitoring the online safety policy including the impact of initiatives. The group will also be responsible for regular reporting to senior leaders and the Governing Board.

The online safety group has the following representative members:

- online safety lead/(s)
- DSL/(s)
- senior leaders
- online safety governor
- technical staff
- teacher and support staff members
- learners
- parents/carers
- community representatives

Members of the online safety group (or other designated group) will assist the online safety lead/(s) (or another relevant person) with:

- the production/review/monitoring of the Federation online safety policy/documents
- the production/review/monitoring of the school filtering procedure (if possible and if the school chooses to have one) and requests for filtering changes
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- reviewing network/filtering/monitoring/incident logs, where possible
- encouraging the contribution of learners to staff awareness, emerging trends and the Federation online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

3. Education and Curriculum

Pupil online safety curriculum

The Federation:

- has a clear, progressive online safety education programme as part of the computing curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience, building on prior experience;
- programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- will remind pupils about their responsibilities through the pupil acceptable use policy and encourage them to adopt safe and responsible use both within and outside school;
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, data protection and copyright;
- ensures in lessons where internet use is pre-planned, it is best practice that learners are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights.

Staff and governor training

The Federation:

- makes regular up to date training available to staff and governors on online safety issues and each school's/setting's online safety education program, an audit of the online safety training needs of all staff will be carried out regularly.
- makes staff aware that Federation systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with Federation policies when accessing school systems and devices.
- provides, as part of the induction process, all staff with information and guidance on the online safety policy and the Federation's ICT acceptable use policy (staff/governors/visitors).

Parent/Carer awareness and training

The Federation:

- provides information and guidance for parents/carers for online safety in a variety of formats. This will include offering specific online safety evenings, and highlighting online safety through the school websites.
- runs a rolling programme of online safety advice, guidance and training for parents;
- issues parents/carers with up to date guidance on an annual basis.

4. Incident management

The Federation:

- has strict monitoring and application of the online safety policy, including the ICT acceptable use policies and a differentiated and appropriate range of sanctions;
- has clear reporting routes which are understood and followed by all members of the Federation community which are consistent with the Federation safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies;
- actively seeks support from other agencies as needed (i.e. the local authority, UK Safer Internet Centre helpline, CEOP, police, Internet Watch Foundation) in dealing with online safety issues;
- monitors and reports online safety incidents that take place and contribute to developments in policy and practice in online safety within the Federation;
- ensures parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- contacts the police if one of our staff or pupils receives online communication that it considers is particularly disturbing or breaks the law;
- will immediately refer any suspected illegal material to the appropriate authorities – i.e. police, Internet Watch Foundation and inform the LA.

5. Managing IT and Communication System

Internet access, security and filtering

The Federation:

- follows guidelines issued by the Department for Education to ensure that it complies with minimum requirements for filtered broadband provision;
- tracks and itemises all authorised hardware on the networks so that only authorised devices are given access'

- uses a guest portal for all unauthorised and unmanaged devices at Aylsham High School and Bure Valley School.
- actively manages all software on the network so that only authorised software is installed and can execute. Unauthorised and unmanaged software is found and prevented from installation or execution;
- actively manages the security configuration of laptops, workstations and servers using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings;
- continuously acquires, assesses, and takes action on new information in order to identify vulnerabilities, remediate, and minimise the window of opportunity for attackers;
- manages the security lifecycle of all in-house developed and acquired software in order to prevent, detect and correct security weaknesses;
- tracks and controls the security use of wireless local area networks through the use of authorised equipment only and guest networks;
- has capability and manages and controls the processes and tools used to back up critical information properly with a proven system for timely recovery;
- identifies the specific knowledge, skills and abilities needed to support defence of the Federation, develop and ensure these are in place through policies, training, planning and awareness programs;
- establishes, implements and actively manages the processes required to prevent attackers from exploiting vulnerable services and settings such as firewalls, routers and switches through password protection, regular updates, software and NCC support;
- manages, tracks and controls the correct use, assignment and configuration of administrative privileges on computers, networks and applications on a need to know basis;
- ensures that confidential and sensitive date does not transfer outside of the networks without the relevant authority and trust levels in place with a focus on security-damaging data;
- keeps logs of events that could help detect, understand, or recover from an attack;
- actively manages the life-cycle of system and application accounts; their creation, use, dormancy and deletion in order to minimise opportunities for attackers;
- has adequate processes and tools to ensure the privacy and integrity of sensitive information and data including its data protection policy;
- uses robust software to protect the Federation's information and also has an incident response system in place with defined roles, training, communications for quickly discovering an attack or loss of data and reinstatement of the integrity of the network and systems.

Email

The Federation:

- provides staff with an email account for their professional use, e.g. @aylshamhigh, @burevalley, @johngaunt, Alfeducation@ or nsix.org.uk and makes clear personal email should be through a separate account;
- uses anonymous email addresses, for example head@, office@;
- will contact the police if one of its staff or pupils receives an email that it considers is particularly disturbing or breaks the law;
- will ensure that email accounts are maintained and up to date.

Pupils email: (Aylsham High School and Bure Valley School)

- uses each school's provisioned pupil email accounts that can be audited.
- teaches pupils about online safety and 'etiquette' of using email both in school and at home.

Staff email:

- staff will use LA or each school's provisioned email systems for professional purposes.
- may restrict access in school to external personal email accounts.
- will never use email to transfer sensitive staff or pupil personal data unless it is protected with secure encryption. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data/file must be protected with security encryption.

School website

- Each school's website complies with statutory DfE requirements.
- Most material is each school's own work; where other's work is published or linked to, the Federation credits the sources used and states clearly the author's identity or status.
- Photographs of pupils published on the web do not have full names attached unless the Federation has parental permission. The Federation does not use pupils' names when saving images in the file names or in the tags when publishing to each school's website.

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Staff are instructed not to run social network spaces for pupils use on a personal basis or to open up their own spaces to their pupils, but to use each schools' preferred system for such communications.
- The use of each school's/setting's approved social networking will adhere to ICT acceptable use policy (staff/governors/visitors) and the Federation's staff code of conduct.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Pupils are required to sign (where appropriate) and follow our [age appropriate] ICT acceptable use policy (pupil).

.

Parents/Carers:

- Parents/carers are reminded about social networking risks and protocols through the parental acceptable use agreement (AHS/BVS) (Appendix 1) and additional communications materials when required.

6. Data Security

Management information system access and data transfer

- The Federation uses guidance from the Information Commissioner's Office to ensure that it complies with its responsibilities to information rights in school. It ensures that it follows the guidelines of the general data protection regulations and complies with the data protection act.

7. Equipment and Digital Content

Bring Your Own Device Guidance for Staff and Pupils

- The Federation uses guidance from the ICT acceptable use policies and each school's curriculum for ICT.

Digital images and video

In the Federation:

- parental/carer permission is gained for use of digital photographs or video involving their child when their child joins each school;
- pupils are not identified in online photographic materials or include the full names of pupils in the credits of any published Federation produced video materials/DVDs without parental permission;
- the schools may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- Staff sign the Federation's ICT acceptable use policy (staff/governors/visitors) and this includes a clause on the use of personal mobile phones/personal equipment.

Related Policies

This policy should be read in line with:

- Safeguarding including child protection policy
- ICT acceptable use policy (staff, governor and visitors)
- ICT acceptable use policy (pupil)
- Data protection policy
- Staff code of conduct
- Anti-bullying policies
- PSHE policy

Appendix 1

ICT Code of Conduct agreement form: parents/carer

Aylsham Learning Federation

Parent/Carer name:……

Pupil name: ……..

Pupil's registration class: ……

As the parent or carer of the above pupil(s), I grant permission for my child to have access to use the internet, virtual learning environments, school email and other ICT facilities at school.

I know that my child has signed a form to confirm that they will keep to the school's rules for responsible ICT use, outlined in the ICT code of conduct (pupils) policy. I also understand that my child may be informed, if the rules have to be changed during the year. I know that the latest copy is available on the school's website and that further advice about safe use of the internet can be found on the website.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, safe access to email, employing appropriate teaching practice and teaching online safety skills to pupils.

I understand that the school can check my child's computer files, and the websites they visit. I also know that the school may contact me if there are concerns about my child's online safety or online behaviour both at school or in the home environment.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

Parent/Carer signature:……. **Date:**…….