AYLSHAM LEARNING FEDERATION

ONLINE SAFETY POLICY

Policy Reference:	JT/Online Safety	Review Frequency:	1 Year
Issue Number:	02 (26.06.2018)	Next Review Date:	26.06.2019
Author:	J. Tuttle		

Ratified by the Governors' Curriculum Committee on: 26.06.2018

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.

Contents

1. 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 and John of Gaunt Infant and Nursery School with respect to the use of technologies.
- Safeguard and protect the children and staff.
- 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 students/pupils.

The 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

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)

Scope

This policy applies to all members of Aylsham Learning Federation community (including staff, students/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.

Communication

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

- Policy to be posted on each school's website/staffroom/classroom.
- Policy to be part of each school's induction pack for new staff, including information and guidance where appropriate.
- All staff must read and sign the 'ICT code of conduct policy (staff/governors/visitors)' before using any school technology resource.

- Regular updates and training on online safety for all staff, including any revisions to the policy.
- ICT code of conduct policy (staff/governors/visitors and students/pupils) discussed with staff and students/pupils at the start of each year. ICT code of conduct policy (staff/governors/visitors) to be issued to members of each school'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 students/pupils are given information about infringements in use and possible sanctions.
- Designated Safeguarding Lead (DSL) acts 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, or Head of School unless the concern is about the Executive Headteacher in which case the concern is referred to the Chair of Governors.

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.
- 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 students/pupils.

2. Education and Curriculum

Student/Pupil online safety curriculum

This 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;
- will remind students/pupils about their responsibilities through the student/pupil ICT code of conduct policy;
- 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, copyright;
- ensures that staff and students/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

This Federation:

- makes regular up to date training available to staff on online safety issues and each school's online safety education program;
- provides, as part of the induction process, all staff with information and guidance on the online safety policy and the Federation's ICT code of conduct policy (staff/governors/visitors).

Parent/Carer awareness and training

This Federation:

- provides information for parents/carers for online safety on each school's website;
- runs a rolling programme of online safety advice, guidance and training for parents;
- parents/carers are issued with up to date guidance on an annual basis.

3. Incident management

In this Federation:

- there is strict monitoring and application of the online safety policy, including the ICT code of conduct policies and a differentiated and appropriate range of sanctions;
- support is actively sought 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;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the Federation;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the police will be contacted if one of our staff or students/pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – i.e. police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication System

Internet access, security and filtering

In this Federation:

- we follow guidelines issued by the Department for Education to ensure that we comply with minimum requirements for filtered broadband provision;
- we track and itemise all authorised hardware on the networks so that only authorised devices are given access'
- a guest portal is available for all unauthorised and unmanaged devices at Aylsham High School and Bure Valley School.
- we actively manage 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;
- we actively manage 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;

- we continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimise the window of opportunity for attackers;
- we manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect and correct security weaknesses;
- we track and control the security use of wireless local area networks through the use of authorised equipment only and guest networks;
- we have capability and manage and control the processes and tools used to back up critical information properly with a proven system for timely recovery;
- we identify 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;
- we establish, implement and actively manage 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;
- we manage, track and control the correct use, assignment and configuration of administrative privileges on computers, networks and applications on a need to know basis;
- we ensure 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;
- we keep logs of events that could help detect, understand, or recover from an attack;
- We actively manage the life-cycle of system and application accounts; their creation, use, dormancy and deletion in order to minimise opportunities for attackers;
- we have adequate processes and tools to ensure the privacy and integrity of sensitive information and data including our data protection policy.
- we use robust software to protect the Federation's information and also have 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

This Federation:

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

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

- We use each school's provisioned pupil email accounts that can be audited.
- Students/Pupils are taught about the online safety and 'netiquette' 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.
- Access in school to external personal email accounts may be blocked.

- Never use email to transfer 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 web site complies with statutory DfE requirements.
- Most material is each school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- Photographs of students/pupils published on the web do not have full names attached unless we have parental permission. We do not use students/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.
- Teachers are instructed not to run social network spaces for students/pupils use on a personal basis or to open up their own spaces to their students/pupils, but to use each schools' preferred system for such communications.
- The use of each school's approved social networking will adhere to ICT code of conduct policy (staff/governors/visitors) and Federation's staff code of conduct.

Students/Pupils: (Aylsham High School and Bure Valley School)

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students/pupils are required to sign and follow our [age appropriate] ICT code of conduct policy (student/pupil).

.

Parents/Carers:

- Parents/carers are reminded about social networking risks and protocols through our parental ICT code of conduct agreement (Appendix 1) and additional communications materials when required.

5. Data Security

Management information system access and data transfer

- We use guidance from the Information Commissioner's Office to ensure that we comply with our responsibilities to information rights in school. We ensure that we follow the guidelines of the general data protection regulations and comply with the data protection act.

6. Equipment and Digital Content

Bring Your Own Device Guidance for Staff and Pupils

- We use guidance from The Education Network (NEN) around Bring Your Own Device and each school's curriculum for ICT.

Digital images and video

In this Federation:

- we gain parental/carer permission for use of digital photographs or video involving their child when their daughter/son joins each school;
- we do not identify students/pupils in online photographic materials or include the full names of students/pupils in the credits of any published Federation produced video materials/DVDs without parental permission;
- Staff sign the Federation’s ICT code of conduct 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 code of conduct staff, governor and visitor policy
- ICT code of conduct student/pupil policy
- Data protection policy
- Staff code of conduct policy
- Anti-bullying policies
- PSHE policy

Appendix 1

ICT Code of Conduct agreement form: parents/carer

Aylsham Learning Federation

Parent/Carer name:………………………………………………………….

Student/Pupil name: ……………………………………………………..

Student/Pupil's registration class: ………………………………………

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

I know that my son/daughter 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 (students/pupils) policy I also understand that my son/daughter 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 students/pupils safe and to prevent students/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 students/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 son/daughter's online safety or online behaviour.

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:**…………………