Bolton
Council

Online Safety Policy

June 2021

Appendices

Appendix	
1	Responding to incidents of misuse – flowchart
2	School Technical Security Policy
3	AUP documents
4	Online Incident Report Log

Development / Monitoring / Review of this Policy

This Online policy has been developed by a working group made up of:

- *Head teacher*
- *Safeguarding Lead*
- *Computing Subject lead*
- *Staff – including Teachers, Support Staff, Technical staff*
- *Governing Body*
- *Parents and Carers*

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This Online policy was approved by the Governing Body *on:*	Summer term 2 (2021)
The implementation of this Online policy will be monitored by the:	Computer Subject Leader Safeguarding Lead Head Teacher
Monitoring will take place at regular intervals:	Annually
Governing Body will receive a report on the implementation of the Online policy generated by the monitoring group (which will include anonymous details of Online incidents) at regular intervals:	Once a year at a Standards Committee
The Online Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new	Summer term 2 (2022)

threats to Online or incidents that have taken place. The next anticipated review date will be:	
Should serious Online incidents take place, the following external persons / agencies should be informed:	David Glyn-Jones – Head Teacher Deborah Helme – School DSL Kerry Hutton – Computing Leader Kelly Stark – Computing Leader Hudsen Daniel-Sam– Chair of Governors LADO Police **See Appendix1**

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of stakeholders – staff, pupils, parents

Rationale

At **Highfield** we strive to ensure that all students remain safe and free from harm and we are committed to playing a full and active part in keeping children safe online. We recognise that we are an important part of the wider safeguarding system for children and young people. The purpose of this document is to ensure that **all** our staff are aware of the arrangements that we have in place for keeping children safe online. It provides guidance to help staff who may have concerns about the online safety or welfare of a child or young person and sets out our position in relation to aspects of the Safeguarding and Child Protection process, when dealing with online safety.

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils / pupils, volunteers, parents / carers, visitors) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Anti-Bullying and Behaviour Policy.

The school 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 behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Online Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing body receiving regular information about online incidents and *monitoring reports. Ideally, a member of the Governing body will take on the role of Online Governor:* The role of the Online Governor will include:

- Regular meetings with the Computing leader
- Regular monitoring of online incident logs
- Regular monitoring of filtering
- Reporting to governing body
- Attend training for online safety where appropriate

Head teacher:

The Head teacher has a duty of care for ensuring the safety (including Online) of members of the school community, though the day to day responsibility for online safety will be delegated to the computing leader.

- The Head teacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious online allegation being made against a member of staff (**See Appendix1**).
- The Head teacher / Senior Leaders are responsible for ensuring that the Computing and other relevant staff receive suitable training to enable them to carry out their online roles and to train other colleagues, as relevant.
- The Head teacher 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 monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
    - ➢ Dedicated subject leader time – at least one day per term to monitor online safety in school and at home
    - ➢ Staff training to keep up-to-date with current policies, procedures, strategies and technology
    - ➢ Regular time for subject leader to liaise with computing technician
- The Senior Leadership Team will receive regular monitoring reports from the Computer leader.

Computing / Online Safety subject leader role:

The role and responsibilities of this position include:

- lead the online group
- take day to day responsibility for online issues and take a leading role in establishing and reviewing the school online policies / documents

- ensure that all staff are aware of the procedures that need to be followed in the event of an online incident taking place
- provide training and advice for staff
- liaise with the Local Authority / relevant body
- liaise with school technical staff
- receive reports of online incidents and create a log of incidents to inform future online development
- meets regularly with online Governor to discuss current issues, review incident logs and filtering / change control logs
- Reports regularly to Senior Leadership Team

School Network – provided and support by Bolton Schools ICT (SICT)

Bolton Schools ICT (SICT) is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required online technical requirements and any Local Authority / other relevant body Online Policy / Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- The filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (See Appendix 2 – HMI document)
- That they keep up to date with online technical information in order to effectively carry out their online role and to inform and update others as relevant
- that the use of the network / internet / online learning environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher, Computing subject leader and DSL for investigation / action / sanction

Teaching, support staff and volunteers

It is essential that all staff:

- receive online safety training and understand their responsibilities
- all new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.

All teaching, support staff and volunteers are responsible for ensuring that:

- They have an up to date awareness of online matters and of the current school online policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy (Appendix 3)
- They report any suspected misuse or problem to the Computing Lead, who will then pass this to the SLT for investigation / action / sanction
- All digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- Online issues are embedded in all aspects of the curriculum
- Pupils understand and follow their age-appropriate acceptable user policy
- Staff should act as good role models in their use of digital technologies the internet and mobile devices

- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations will be discussed with children at appropriate times they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices in lessons where internet use is pre-planned. Pupils 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

Designated Safeguarding Lead

The DSL will be trained in online issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying
- Peer on peer abuse.
- Sexting

Online Group

At Highfield School the Online Group consists of the following people: Designated Safeguarding Lead, Computer Leader, Onsite Manager, and nominated governor.
The Online Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online and the monitoring the online policy including the impact of initiatives. The group will be responsible for regular reporting to the Governing Body.

Pupils:

- Understand and follow their age-appropriate acceptable user policy (Appendix 3)
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (with age appropriate vocabulary and when needed)
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good online practice when using digital technologies out of school and realise that the school's online policy covers their actions out of school, if related to their membership of the school
- Will be expected to know and understand policies on remote learning and the rules surrounding remote lessons.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through:

- Parents' evenings, newsletters, emails, website and information about national / local online safety campaigns / literature.

Parents and carers will be encouraged to support the school in promoting good online practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Their children's personal devices in the school (where this is allowed)

Parents and carers will be encouraged to know and understand policies on remote learning and the expectations of behaviour during remote lessons.

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's teaching. Children and young people need the help and support of the school to recognise and avoid online risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and lessons throughout the year.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the age-appropriate AUP and encouraged to adopt safe and responsible use both within and outside school

Education – parents / carers

Many parents and carers have only a limited understanding of the online risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site - reference to the relevant web sites / publications
-

- Parents / Carers evening workshops
- High profile events / campaigns e.g. Safer Internet Day

Technical – infrastructure / equipment, filtering and monitoring

For school supported by Bolton Schools ICT:

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online responsibilities:

- School technical systems will be managed and reviewed annually in ways that ensure that the school meets recommended technical requirements
- All users will have clearly defined access rights to school technical systems and devices.
- All school network users will be assigned a username and password by Bolton Schools ICT who for at the appropriate level of access needed for their role.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- Bolton Schools ICT provide a platform where school should report any inappropriate content accessible in school
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. 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 virus software (Appendix 2).

An agreed policy is in place that states:

- staff members only are allowed on school devices that may be used out of school.
- All devices must be used for school purposes only
- staff are forbidden from downloading executable files and installing programmes on school devices.
- The use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices is now prohibited and all staff must store and send data via the school's secure office 365 system
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured in line with GDPR recommendations.

Data Privacy

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data in line with GDPR recommendations.

The **school** must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Privacy Policy
- It is registered as a Data Controller for the purposes of the GDPR legislation
- Responsible persons are appointed / identified – Chief Privacy Officer
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Privacy clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud environments which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

If personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, chat) must be professional in tone and content. These communications may only take place on official

(monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

- Pupils should be taught about online issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. **Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'**. While, Ofsted's Online framework 2012, reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:
Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the SLT and online group to ensure compliance with the school policies. The acceptable use policy will be shared with staff annually to ensure up to date knowledge and understanding of this information. At Highfield, we will follow the guidelines set out in the Guidance for Working with Children 2015 document to ensure the protection of professional identity.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. Cyber-bullying, via texts and emails, will be treated as seriously as any other type of bullying and will be managed through our anti-bullying and behaviour policies. We recognise that online abuse will often occur concurrently with face to face abuse. There are a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. However, school feels that there is a need to teach all pupils that certain sites and games have age restrictions to keep them safe and that should they access such sites and games, they may be putting themselves at risk of accessing inappropriate content and cyber-bullying.

Responding to incidents of misuse

This policy is intended for use when staff need to manage incidents that involve the use of misappropriate online content. It encourages a safe and secure approach to the management of incidents. Incidents might involve illegal or inappropriate activities (See Appendix 4).

Should we have any concerns we will:
· Refer to the Department of Education guidance on Teaching on line safety in schools (June 2019), Greater Manchester Procedures and UK Council for child internet safety (UKCCIS).
· Report to CEOP a law enforcement agency that keeps children and young people safe from sexual exploitation and abuse- Reporting link or tel 0800 1111
https://www.thinkuknow.co.uk/
https://www.ceop.police.uk/Safety-Centre/

We access resources from safer Internet to keep students safe online. We will also encourage our students/parents/carers to anonymously report online child sexual abuse imagery and videos to the safer internet Hotline.
· Report any harmful content to - www.reportharmfulcontent.com

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart for responding to online safety incidents and report immediately to the police (See Appendices 1 and 4).

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.
In the event of suspicion, all steps in this procedure should be followed:

Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
It is important to ensure that the relevant staff should 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 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 (except in the case of images of child sexual abuse – see below)
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
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include: incidents of 'grooming' behaviour the sending of obscene materials to a child adult material which potentially breaches the Obscene Publications Act criminally racist material other criminal conduct, activity or materials. Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.