****

2

*Walton-le-Dale High School*

Online Safety Policy

**Development / Monitoring / Review of this Policy**

4

This Online Safety policy has been developed by Senior Leaders; Online Safety Coordinator; Staff; Governors; Students. A safe guarding issue is one where technology is used. Updated in light of KCSIE 2015 and KCSIE 2016. Please note the term ‘online safety now replaces ‘esafety’

**Schedule for Development / Monitoring / Review**

5

|  |  |
| --- | --- |
| This Online Safety policy was approved by the *Governing Body / Governors Sub Committee:* | *2014* |
| The implementation of this Online Safety policy will be monitored by the: | *Senior Leadership Team*  *Designated Senior Leader: Child Protection and Safeguarding*  *Head of ICT* |
| Monitoring will take place at regular intervals: | *In line with CP policy or as and when needed* |
| The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online Safety or incidents that have taken place. The next anticipated review date will be: | *May 2017* |
| Should serious Online Safety incidents take place, the following external persons / agencies should be informed: | *LA Child Protection Officer, LADO; Police; CEOP as appropriate* |

The school will monitor the impact of the policy using:

• Logs of reported incidents

• Monitoring logs of internet activity (including sites visited)

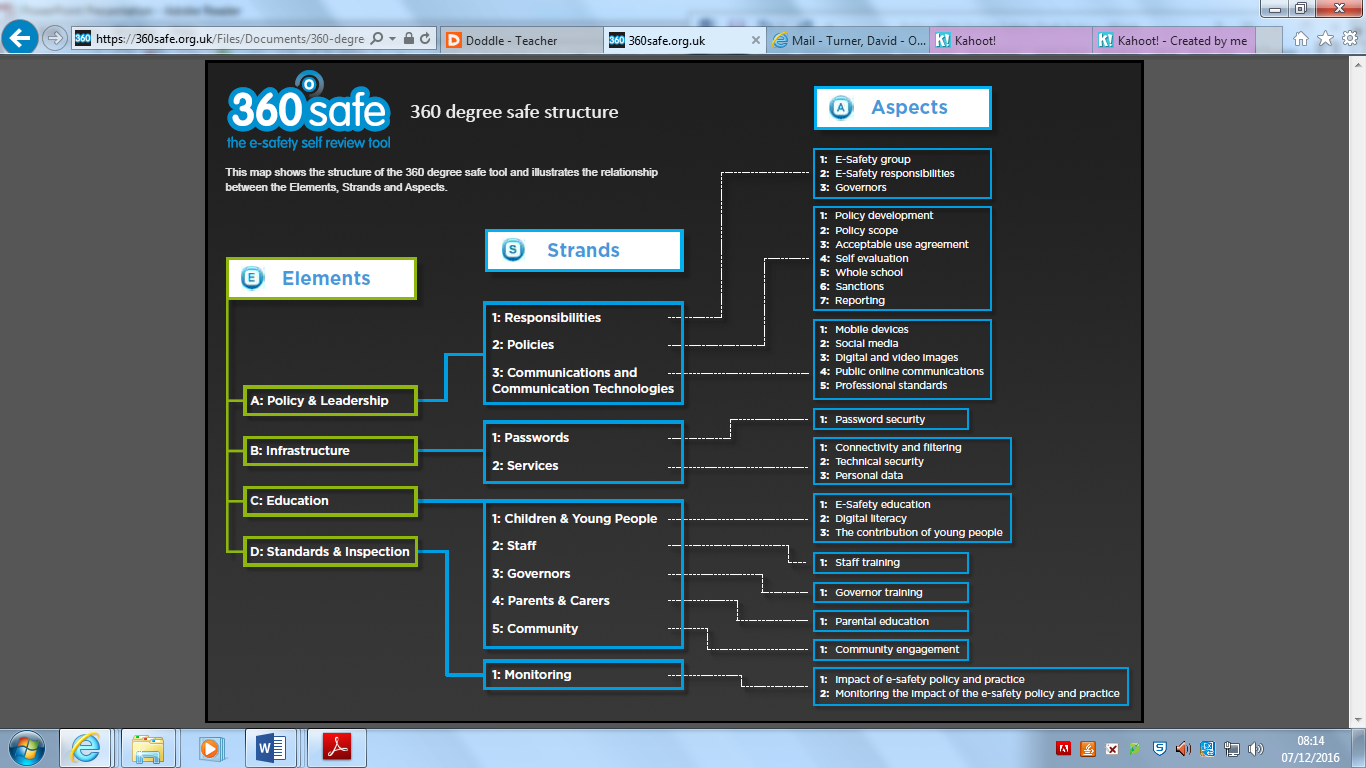
• Internal monitoring data for network activity

• Surveys / questionnaires of students, parents / carers and staff

**Scope of the Policy**

6

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

This map shows the structure of the 360 degree safe tool and illustrates the elements, strands and aspects of online safety within Walton le Dale High School.

The Education and Inspections Act 2006 empowers Head Teachers to such extent as is reasonable, to regulate the behaviour of students 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 Safety incidents covered by this policy, which may take place outside of the school / academy, 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 Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying   
policies and will, where known, inform parent and carers of incidents of inappropriate Online Safety   
behaviour that take place out of school.

**Roles and Responsibilities**

7

The following section outlines the Online Safety roles and responsibilities of individuals and groups within the school:

**Governors:**

All governors must be familiar with the statutory requirements of ‘Keeping Children Safe In Education 2015 and 2016.’ (KCSIE 2016 and KCSIE 2015). Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors after receiving regular information about Online Safety incidents and monitoring reports. A member of the Governing Body. The role of the Online Safety Governor will include:   
  
• meetings with the Online Safety Co-ordinator

• monitoring of Online Safety incident logs

• regular monitoring of filtering / change control logs

• Undertaking regular and appropriate safety training.  
• reporting to relevant Governors meetings

**Head Teacher and Senior Leaders:**

• The Head Teacher has a duty of care for ensuring the safety (including Online Safety) of members of the school community, though the day to day responsibility for Online Safety will be delegated to the Designated Safeguarding Person who in turn delegates to the Online Safety Co-ordinator.

• The Head Teacher 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. (See flow chart on dealing with Online Safety incidents).

• The Head Teacher is responsible for ensuring that the Designated Safeguarding Person, Online Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their Online Safety 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 Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

**Online Safety Coordinator:**

• leads the Online Safety committee

• takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents

• ensures that all staff are aware of the procedures that need to be followed in the event of an

Online Safety incident taking place.

• provides training and advice for staff

• liaises with the DSP who liaises with the Local Authority

• liaises with school technical staff

• receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments

• meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs

• attends relevant meeting / committee of Governors

**Network Manager / Technical staff:**

The Network Manager 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 Safety technical requirements and any Local Authority / other relevant body Online Safety 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 is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person

• that 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

• that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head Teacher or Designated Safeguarding Person for investigation / action / sanction

• that monitoring software / systems are implemented and updated as agreed in school policies

**Teaching and Support Staff**

Teaching and support staff are responsible for ensuring that:

• they have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices

• they have read, understood and signed the Staff Acceptable Use Policy (AUP)

• they report any suspected misuse or problem to the Head Teacher or Designated Safeguarding Person for investigation / action / sanction

• all digital communications with students/ parents / carers should be 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

• students understand and follow the Online Safety and acceptable use policies

• students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

• 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 students 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

**Safeguarding Designated Person - Child Protection**

The DSP should be trained in Online Safety 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

**Online Safety Group**

The Online Safety Group is a sub-group of the ICT Development Group. It provides a consultative group that has wide representation from the school staff, with responsibility for issues regarding Online Safety and the monitoring the Online Safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body via the Online Safety Co-ordinator.

Members of the Online Safety Group (or other relevant group) will assist the Designated Safeguarding   
Person with:

• the production / review / monitoring of the school Online Safety policy.

• the production / review / monitoring of the school filtering policy and requests for filtering changes.

• mapping and reviewing the Online Safety curricular provision – ensuring relevance, breadth and progression

• monitoring network / internet / incident logs

• consulting stakeholders – including parents / carers and the students about the Online Safety provision

Students:

**•** are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy

• have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

• 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 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 / 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, letters, website / VLE and information about

national / local Online Safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good Online Safety practice and to follow guidelines on the appropriate use of:

• digital and video images taken at school events

• access to parents’ sections of the website / VLE and on-line student / student records

• their children’s personal devices in the school(where this is allowed)

• Training will be made available to parents on online safety

Community Users

Community Users who access school systems / website / VLE as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

11

Policy Statements

Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in Online Safety is therefore an essential part of the school’s Online Safety provision. Children and young people need the help and support of the school to recognise and avoid Online Safety risks and build their resilience. (KCSIE 2016 and KCSIE 2015).

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 tutorial / pastoral activities

• Students 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.

• Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

• Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school

• Staff should act as good role models in their use of digital technologies the internet and mobile devices

• in lessons where internet use is pre-planned, it is best practice that students 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 students 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, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff 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.

Education – parents / carers

Many parents and carers have only a limited understanding of Online Safety 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, VLE

• Parents / Carers evenings / sessions

• High profile events / campaigns eg Safer Internet Day

• Reference to the relevant web sites / publications through Moodle eg [www.swgfl.org.uk](http://www.swgfl.org.uk) [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/) <http://www.childnet.com/parents-and-carers>

Education & Training – Staff / Volunteers

It is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

• Formal Online Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the Online Safety training needs of all staff will be carried out regularly.

• 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.

• The Designated Safeguarding Person/Online Safety Co-ordinator will receive regular updates through attendance at external training events (eg from LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.

• This Online Safety policy and its updates will be presented to and discussed by staff in staff in either team meetings / INSET days.

• The Online Safety Coordinator / Designated Safeguarding Person will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in Online Safety training / awareness sessions, with particular   
importance for those who are members of any sub-committee involved in technology / Online Safety / health and safety / child protection. This may be offered in a number of ways:

• Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation .

• Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

All governors will understand their statutory duties under (KCSIE 2016 and KCSIE 2015).

Technical – infrastructure / equipment, filtering and   
monitoring

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 Safety responsibilities:

• School technical systems will be managed in ways that ensure that the school meets recommended technical requirements (these may be outlined in Local Authority / other relevant body policy and guidance)

• There will be regular reviews and audits of the safety and security of school academy technical systems

• Servers, wireless systems and cabling must be securely located and physical access restricted

• All users will have clearly defined access rights to school technical systems and devices.

• All users will be provided with a username and secure password by the network manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every term. (

• The “master / administrator” passwords for the school ICT system, used by the Network Manager must also be available to the Head Teacher or other nominated senior leader and kept in a secure place (eg school safe)

• The network manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs.

* 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 (see appendix for more details)

• The school has provided enhanced user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / students / students etc)

• School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.

• An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).

• 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.

• An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems.

• An agreed policy is in place regarding the extent of personal use that users (staff / students/ community users) and their family members are allowed on school devices that may be used out of school.

• An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

### **Appropriate Filtering**

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

### **Illegal Online Content**

In considering filtering providers or systems , network manager and teachers should ensure that access to illegal content is blocked, specifically that the filtering providers:

Are IWF members and block access to illegal Child Abuse Images and Content (CAIC)

Integrate the ‘the police assessed list of unlawful terrorist content, produced on behalf of the Home Office’.

### **Inappropriate Online Content**

Recognising that no filter can guarantee to be 100% effective, schools should be satisfied that their filtering system manages the following content (and web search)

* Discrimination: Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.
* Drugs / Substance abuse: displays or promotes the illegal use of drugs or substances
* Extremism: promotes terrorism and terrorist ideologies, violence or intolerance
* Malware / Hacking: promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
* Pornography: displays sexual acts or explicit images
* Piracy and copyright theft: includes illegal provision of copyrighted material
* Self Harm: promotes or displays deliberate self harm (including suicide and eating disorders)
* Violence: Displays or promotes the use of physical force intended to hurt or kill

This list should not be considered an exhaustive list and providers will be able to demonstrate how their system manages this content and many other aspects

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions

### **Filtering System Features**

Additionally the network manager and teachers should consider that their filtering system meets the following principles

* Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role
* Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content
* Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking
* Identification - the filtering system should have the ability to identify users
* Mobile and App content – isn’t limited to filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies
* Multiple language support – the ability for the system to manage relevant languages
* Network level - filtering should be applied at ‘network level’ ie, not reliant on any software on user devices
* Reporting mechanism – the ability to report inappropriate content for access or blocking
* Reports – the system offers clear historical information on the websites visited by your users

Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to [“consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum”.](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2)

**Bring Your Own Device (BYOD)**

The educational opportunities offered by mobile technologies are being expanded as a wide range   
of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of Online Safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

* The school has a set of clear expectations and responsibilities for all users
* The school adheres to the Data Protection Act principles
* All users are provided with and accept the Acceptable Use Agreement
* All network systems are secure and access for users is differentiated
* Where possible these devices will be covered by the school’s / academy’s normal filtering systems, while being used on the premises
* All users will use their username and password and keep this safe
* Mandatory training is undertaken for all staff
* Students receive training and guidance on the use of personal devices
* Regular audits and monitoring of usage will take place to ensure compliance
* Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
* Any user leaving the school will follow the process outlined within the BYOD policy

Use of digital and video images

* Please refer to the Child Protection Policy for use of personal mobiles with cameras for school use.

**USE OF MOBILE PHONES AND CAMERAS**

In 2012 new regulations were introduced in to Early Years settings. The following is included as best practice with respect to the EYFS regulations and being adapted for use in a high school setting.

Staff, visitors and volunteers are not permitted to use their own mobile phones, tablets/i-pads to take or record any images of students for their own records during session times.

Where students take photographs of other students it is only with consent.

**Consent**

* Under the Data Protection Act 1998, the school must seek parental consent to take photographs and use video recorders or other technological means.
* This consent is sought annually as family situations may change.
* It will be made clear to parents/carers that if they consent their child’s image may appear on the School website or in the School Prospectus or other external marketing means eg banners etc. When this is the case, when practicable, parents/carers will be informed that this may be happening.
* If a parent does not give that consent then all possible means must be made to ensure that their child is never knowingly photographed/filmed. It is however, acknowledged that occasionally their child might by mistake be in the background of a picture.
* A list of all students whose image must not be taken will be on the Staff room wall main noticeboard.

**Procedures**

The word ‘photograph’ is used to indicate all images whether still or moving.

* All photographs will be stored In the SIMS ‘Staff Only’ folder which is password protected
* The schools’ digital camera/s or memory cards etc must not leave the school setting unless on an official school trip.
* Photos are printed/uploaded in the school by staff and once done images are then immediately removed from the cameras memory or other device eg card. When possible it is advisable to have another member of staff witness that the photos have been deleted.
* Printed photographs or images may be used in wall displays or in coursework. If a student objects to this use the school will respect their wishes and remove them.
* At school events, such as Presentation evenings etc where students are fully clothed it will be quite acceptable for parents/carers to take photographs of their children. However, at certain events eg productions or sporting events parents will be requested not to use their own cameras.
* Many staff will have personal mobile phones with inbuilt cameras. These should not be used during the school sessions for personal use except in emergencies and the camera element should not be used.
* There may be exceptional cases when a member of staff does use the camera element of their mobile phone eg if taking a photo of an intruder, car number plate or some other circumstance where the photo would be used to provide evidence for a police enquiry.

Cameras and mobile phones are prohibited in all toilet areas

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

• When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.

• In accordance with guidance from the Information Commissioner’s Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.

• Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

• Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

• Students must not take, use, share, publish or distribute images of others without their permission

• Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

• Students’ full names will not be used anywhere on a website or blog, particularly in association with photographs.

• Written permission from parents or carers will be obtained before photographs of students are published on the school website

• Student’s work can only be published with the permission of the student / student and parents or carers.

Data Protection

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.

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.
* It has a Data Protection Policy.
* It is registered as a Data Controller for the purposes of the Data Protection Act (DPA).
* Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs).
* Risk assessments are carried out.
* 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 Protection clauses in all contracts where personal data may be passed to third parties
* There are clear policies about the use of cloud storage / cloud computing 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.

When 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 (many memory sticks / cards and other mobile devices cannot be password protected).

• the device must offer approved virus and malware checking software

16

• 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

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | Staff & other  adults | | | Students / Students | | | | |
| Communication Technologies | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| Mobile phones may be brought to school |  |  |  |  |  |  |  |  |
| Use of mobile phones in lessons |  |  |  |  |  |  |  |  |
| Use of mobile phones in social time |  |  |  |  |  |  |  |  |
| Taking photos on mobile phones / cameras |  |  |  |  |  |  |  |  |
| Use of other mobile devices eg tablets, gaming devices |  |  |  |  |  |  |  |  |
| Use of personal email addresses in school, or on school network |  |  |  |  |  |  |  |  |
| Use of school email for personal emails |  |  |  |  |  |  |  |  |
| Use of messaging apps |  |  |  |  |  |  |  |  |
| Use of social media |  |  |  |  |  |  |  |  |
| Use of blogs |  |  |  |  |  |  |  |  |

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 students should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).

• **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 students or parents / carers (email, chat, VLE etc) 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.

• Whole class / group email addresses and above will be provided with individual school email addresses for educational use.

• Students should be taught about Online Safety 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

All schools, academies and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools/academies 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 minimize risk of harm to students, 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.
* Clear reporting guidance, including responsibilities, procedures and sanctions
* Risk assessment, including legal risk

School staff should ensure that:

* No reference should be made in social media to students / students, 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 senior risk officer and Online Safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

### **Social Media Policy introduction**

1.1The internet provides a range of web & social media tools that allow users to interact with one another, for example from rediscovering friends on social networking sites such as *Facebook* to keeping up with other people’s lives on *Twitter* and maintaining pages and content on websites and on internet encyclopaedias such as *Wikipedia*.

1.2While recognising the benefits of these media for new opportunities for communication, this policy sets out the principles that Walton-le-Dale staff and contractors are expected to follow when using social media.

1.3 It is crucial that pupils, parents and the public at large have confidence in the school’s decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of pupils and other staff and the reputation of the school is safeguarded.

1.4 Staff members must be conscious at all times of the need to keep their personal and professional lives separate.

### **2 Social Media Policy scope**

2.1 This policy applies to Walton-le-Dale’s governing body, all teaching and other staff, whether employed by the County Council or employed directly by the school, external contractors providing services on behalf of the school or the County Council, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to as ‘staff members’ in this policy.

2.2 This policy covers personal use of website and social media as well as the use of websites and social media for official school purposes, including sites hosted and maintained on behalf of the school (see sections 5, 6, 7 and Appendices A and B).

2.3 This policy applies to personal webspace such as social networking sites (for example *Facebook*, *MySpace*), blogs, microblogs such as *Twitter*, chatrooms, forums, podcasts, open access online encyclopaedias such as *Wikipedia,* social bookmarking sites such as *Pintrest* and content sharing sites such as *flickr* and *YouTube*. The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media - the principles set out in this policy must be followed irrespective of the medium.

**3 LEGAL FRAMEWORK**

3.1 Walton-le-Dale High School is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of the school are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional codes of conduct, including:

* + - the Human Rights Act 1998
    - Common law duty of confidentiality, and
    - the Data Protection Act 1998.

3.2 Confidential information includes, but is not limited to:

* Person-identifiable information, e.g. pupil and employee records protected by the Data Protection Act 1998
* Information divulged in the expectation of confidentiality
* School business or corporate records containing organisationally or publicly sensitive information
* Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and
* Politically sensitive information.

3.3 Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

* Libel Act 1843
* Defamation Acts 1952 and 1996
* Protection from Harassment Act 1997
* Criminal Justice and Public Order Act 1994
* Malicious Communications Act 1998
* Communications Act 2003, and
* Copyright, Designs and Patents Act 1988.

3.4 Walton-le-Dale High School and the County Council could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff members who harass co-workers online or who engage in cyberbullying or discrimination on the grounds of race, sex, disability, etc or who defame a third party while at work may render Walton-le-Dale High School or the County Council liable to the injured party.

**4 RELATED POLICIES**

4.1 This policy should be read in conjunction with appropriate policies related to staff conduct.

**5 PRINCIPLES – BE PROFESSIONAL, RESPONSIBLE AND RESPECTFUL**

5.1 You must be conscious at all times of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between your work for the school and your personal interests.

5.2 You must not engage in activities involving websites or social media which might bring Walton-le-Dale High School into disrepute.

5.3 You must not represent your personal views as those of Walton-le-Dale High School on any social medium.

5.4 You must not discuss personal information about pupils, Walton-le-Dale High School staff and other professionals you interact with as part of your job on websites or social media.

5.5 You must not use websites or social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations or Walton-le-Dale High School.

5.6 You must be accurate, fair and transparent when creating or altering online sources of information on behalf of Walton-le-Dale High School.

**6** **PERSONAL USE OF SOCIAL MEDIA**

6.1 Staff members must not identify themselves as employees of Walton-le-Dale High School or service providers for the school in their personal webspace. This is to prevent information on these sites from being linked with the school and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services.

6.2 Staff members must not have contact through any personal social medium with any pupil, whether from Walton-le-Dale High School or any other school, unless the pupils are family members.

6.3 Walton-le-Dale High School does not expect staff members to discontinue contact with their family members via personal social media once the school starts providing services for them. However, any information staff members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way.

6.4 Staff members must not have any contact with pupils’ family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.

6.5 If staff members wish to communicate with pupils through social media sites or to enable pupils to keep in touch with one another, they can only do so with the approval of the school and through official school sites created according to the requirements specified in section 7 and Appendix A.

6.6 Staff members must decline ‘friend requests’ from pupils, or ex-pupils under the age of 18, that they receive in their personal social media accounts. Instead, if they receive such requests from pupils who are not family members, they must discuss these in general terms in class and signpost pupils to become ‘friends’ of the official school site.

6.7 On leaving Walton-le-Dale High School’s service, staff members must not contact Walton-le-Dale High School’s pupils by means of personal social media sites. Similarly, staff members must not contact pupils from their former schools by means of personal social media.

6.8 Information staff members have access to as part of their employment, including personal information about pupils and their family members, colleagues, staff and other parties and school information must not be discussed on their personal webspace.

6.9 Photographs, videos or any other types of image of pupils and their families or images depicting staff members wearing school uniforms or clothing with school logos must not be published on personal webspace.

6.10 School email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

6.11 Staff members must not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the employer’s IP address and the intervention will, therefore, appear as if it comes from the employer itself.

6.12 Walton-le-Dale High School logos or brands must not be used or published on personal webspace.

6.13 Walton-le-Dale High School only permits limited personal use of social media while at work. Staff members are expected to devote their contracted hours of work to their professional duties and, in practice, personal use of the internet should not be on the school’s time.

6.14 Caution is advised when inviting work colleagues to be ‘friends’ in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the work place.

6.15 Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

**7 USING SOCIAL MEDIA ON BEHALF OF WALTON-LE-DALE HIGH SCHOOL**

## 7.1 Staff members can only use official school sites for communicating with pupils or to enable pupils to communicate with one another.

## 7.2 There must be a strong pedagogical or business reason for creating official school sites to communicate with pupils or others. Staff must not create sites for trivial reasons which could expose the school to unwelcome publicity or cause reputational damage.

## 7.3 Official school sites must be created only according to the requirements specified in Appendix A of this Policy. Sites created must not breach the terms and conditions of social media service providers, particularly with regard to minimum age requirements.

## 7.4 Staff members must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

**8 MONITORING OF INTERNET USE**

8.1 Walton-le-Dale High Schoolmonitors usage of its internet and email services without prior notification or authorisation from users.

8.2 Users ofWalton-le-Dale High School’semail and internet services should have no expectation of privacy in anything they create, store, send or receive using the school’s ICT system.

**9 BREACHES OF THE POLICY**

9.1 Any breach of this policy may lead to disciplinary action being taken against the staff member/s involved in line with Walton-le-Dale High SchoolDisciplinary Policy and Procedure.

9.2 A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of Walton-le-Dale High School or any illegal acts or acts that render Walton-le-Dale High School liable to third parties may result in disciplinary action or dismissal.

9.3 Contracted providers of Walton-le-Dale High School services must inform the relevant school officer immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the school. Any action against breaches should be according to contractors’ internal disciplinary procedures.

**Unsuitable / inappropriate activities**

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| User Actions  18 | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
| **Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:** | **Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978. This includes sexting by minors or teachers** |  |  |  |  | X |
| **Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.** |  |  |  |  | X |
| **Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008** |  |  |  |  | X |
| **criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986** |  |  |  |  | X |
| **pornography** |  |  |  | X |  |
| **promotion of any kind of discrimination** |  |  |  | X |  |
| **threatening behaviour, including promotion of physical violence or mental harm** |  |  |  | X |  |
| **any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute** |  |  |  | X |  |
| **Using school systems to run a private business** | |  |  |  | X |  |
| **Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy** | |  |  |  | X |  |
| **Infringing copyright** | |  |  |  | X |  |
| **Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)** | |  |  |  | X |  |
| **Creating or propagating computer viruses or other harmful files** | |  |  |  | X |  |
| **Unfair usage (downloading / uploading large files that hinders others in their use of the internet)** | |  |  |  | X |  |
| **On-line gaming (educational)** | | X |  |  |  |  |
| **On-line gaming (non educational)** | | X |  |  |  |  |
| **On-line gambling** | |  |  |  |  | X |
| **On-line shopping / commerce** | |  |  |  | X |  |
| **File sharing** | | X |  |  |  |  |
| **Use of social media** | |  |  |  | X |  |
| **Use of messaging apps** | |  |  |  | X |  |
| **Use of video broadcasting eg Youtube**  19 | | X |  |  |  |  |

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

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 (below and appendix) for responding to online safety incidents and report immediately to the police.**



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 / volunteer 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 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 (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.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Students / Students | Actions / Sanctions | | | | | | | | |
| Incidents: | Refer to class teacher / tutor | Refer to Head of Department / Head of Year / other | Refer to Head Teacher | Refer to Police | Refer to technical support staff for action re filtering / security etc | Inform parents / carers | Removal of network / internet access rights | Warning | Further sanction eg detention / exclusion |
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** |  | X | X | X |  |  |  |  |  |
| Unauthorised use of non-educational sites during lessons | X | X |  |  | X | X | X | X | X |
| Unauthorised use of mobile phone / digital camera / other mobile device | X | X |  |  | X | X | X | X | X |
| Unauthorised use of social media / messaging apps / personal email | X | X |  |  | X | X | X | X | X |
| Unauthorised downloading or uploading of files | X | X |  |  | X | X | X | X | X |
| Allowing others to access school network by sharing username and passwords | X | X |  |  | X | X | X | X | X |
| Attempting to access or accessing the school network, using another student’s / student’s account | X | X | X |  | X | X | X | X | X |
| Attempting to access or accessing the school network, using the account of a member of staff | X | X | X |  | X | X | X | X | X |
| Corrupting or destroying the data of other users | X | X | X |  | X | X | X | X | X |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | X | X |  |  | X | X | X | X | X |
| Continued infringements of the above, following previous warnings or sanctions | X | X | X |  | X | X | X | X | X |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | X | X | X |  | X | X | X | X | X |
| Using proxy sites or other means to subvert the school’s / academy’s filtering system | X | X | X |  | X | X | X | X | X |
| Accidentally accessing offensive or pornographic material and failing to report the incident | X | X | X |  | X | X | X | X | X |
| Deliberately accessing or trying to access offensive or pornographic material | X | X | X |  | X | X | X | X | X |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act  21 | X | X | X | X | X | X | X | X | X |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Staff | Actions / Sanctions | | | | | | | | | |
| Incidents: | | Refer to line managerr | Refer to Head Teacher | Refer to Local Authority / HR | Refer to Police | Refer to Technical Support Staff for action re filtering etc | Warning | Suspension | Disciplinary action |
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** | | X | X | X | X | X | X | X | X |
| Inappropriate personal use of the internet / social media / personal email | | X | X |  |  | X | X | X | X |
| Unauthorised downloading or uploading of files | | X | X |  |  | X | X | X | X |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person’s account | | X | X |  |  | X | X | X | X |
| Careless use of personal data eg holding or transferring data in an insecure manner | | X | X |  |  | X | X | X | X |
| Deliberate actions to breach data protection or network security rules | | X | X | X |  | X | X | X | X |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | | X | X | X | X | X | X | X | X |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | | X | X | X | X | X | X | X | X |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / students | | X | X | X | X | X | X | X | X |
| Actions which could compromise the staff member’s professional standing | | X | X |  |  | X | X | X | X |
| Actions which could bring the schoolinto disrepute or breach the integrity of the ethos of the school | | X | X |  |  | X | X | X | X |
| Using proxy sites or other means to subvert the school’s / academy’s filtering system | | X | X |  | X | X | X | X | X |
| Accidentally accessing offensive or pornographic material and failing to report the incident | | X | X |  |  | X | X | X | X |
| Deliberately accessing or trying to access offensive or pornographic material | | X | X | X | X | X | X | X | X |
| Breaching copyright or licensing regulations | | X | X | X | X | X | X | X | X |
| Continued infringements of the above, following previous warnings or sanctions | | X | X | X | X | X | X | X | X |

22

Sexting

*Keeping Children Safe in Education* statutory guidance sets out that all schools should have an effective child protection policy. Youth produced sexual imagery and a school’s approach to it should be reflected in the policy.

All incidents involving youth produced sexual imagery should be responded to in line with the school’s safeguarding and child protection policy.

When an incident involving youth produced sexual imagery comes to a school or college’s attention:

* The incident should be referred to the DSL as soon as possible
* The DSL should hold an initial review meeting with appropriate school staff
* There should be subsequent interviews with the young people involved (if appropriate)
* Parents should be informed at an early stage and involved in the process unless there is good

reason to believe that involving parents would put the young person at risk of harm

* At any point in the process if there is a concern a young person has been harmed or is at risk of harm a referral should be made to children’s social care and/or the police immediately.

Disclosure

Disclosures about youth produced sexual imagery can happen in a variety of ways. The young person affected may inform a class teacher, the DSL in school, or any member of the school or college staff. They may report through an existing reporting structure, or a friend or parent may inform someone in school or college, or inform the police directly.

Any direct disclosure by a young person should be taken very seriously. A young person who discloses they are the subject of sexual imagery is likely to be embarrassed and worried about the consequences. It is likely that disclosure in school is a last resort and they may have already tried to resolve the issue themselves.

**Initial review meeting**

The initial review meeting should consider the initial evidence and aim to establish:

* Whether there is an immediate risk to a young person or young people
* If a referral should be made to the police and/or children’s social care
* If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
* What further information is required to decide on the best response
* Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
* Whether immediate action should be taken to delete or remove images from devices or online services
* Any relevant facts about the young people involved which would influence risk assessment
* If there is a need to contact another school, college, setting or individual
* Whether to contact parents or carers of the pupils involved - in most cases parents should be involved

An immediate referral to police and/or children’s social care should be made if at this initial stage:

1. The incident involves an adult

2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)

3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person’s developmental stage, or are violent

4. The imagery involves sexual acts and any pupil in the imagery is under 1317

5. You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply then a school may decide to respond to the incident without involving the police or children’s social care (a school can choose to escalate the incident at any time if further information/concerns come to light).

The decision to respond to the incident without involving the police or children’s social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school’s pastoral support and disciplinary framework and if appropriate local network of support.

The decision should be made by the DSL with input from the Headteacher and input from other members of staff if appropriate. The decision should be recorded in line with school policy.

The decision should be in line with the school’s child protection procedures and should be based on consideration of the best interests of the young people involved. This should take into account proportionality as well as the welfare and protection of the young people. The decision should be reviewed throughout the process of responding to the incident.

**Assessing the risks**

The circumstances of incidents can vary widely. If at the initial review stage a decision has been made not to refer to police and/or children’s social care, the DSL should conduct a further review (including an interview with the young people involved) to establish the facts and assess the risks.

When assessing the risks the following should be considered:

Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?

Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?

Are there any adults involved in the sharing of imagery?

What is the impact on the pupils involved?

Do the pupils involved have additional vulnerabilities?

Does the young person understand consent?

Has the young person taken part in this kind of activity before?

**Informing parents (or carers)**

Parents (or carers) should be informed and involved in the process at an early stage unless informing the parent will put the young person at risk of harm. Any decision not to inform the parents would generally be made in conjunction with other services such as children’s social care and/or the police, who would take the lead in deciding when the parents should be informed. DSLs may work with the young people involved to decide on the best approach for informing parents. In some cases DSLs may work to support the young people to inform their parents themselves.

**Reporting incidents to the police**

If it is necessary to refer to the police, contact should be made through existing arrangements. This may be through a safer schools officer, a PCSO (Police Community Security Officer), local neighbourhood police or by dialling 101. Once a report is made to the police, the report has to be recorded and the police will conduct an investigation. This may include seizure of devices and interviews with the young people involved.

**Securing and handing over devices to the police**

If any devices need to be seized and passed onto the police then the device(s) should be confiscated18 and the police should be called. The device should be turned off and placed under lock and key until the police are able to come and retrieve it.

**Children’s social care contact and referrals**

If the DSL is aware that children’s social care are currently involved with a young person involved in an incident of youth produced sexual imagery then they should contact children’s social care. They should also contact children’s social care if they believe they may be involved, or have been involved with a young person in the past. If as a result of the investigation the DSL believes there are wider issues which meet the threshold for children’s social care involvement then they should make a referral in line with their child protection procedures. DSLs should ensure that they are aware of, and familiar with, any relevant local policies, procedures and contact points/names which are available to support schools in responding to youth produced sexual imagery. If a local area has a Multi-Agency Safeguarding Hub (MASH) then this may be the most appropriate place for schools to initially make a referral.

**Searching devices, viewing and deleting imagery**

**Viewing the imagery**

Adults should **not** view youth produced sexual imagery unless there is good and clear reason to do so. Wherever possible responses to incidents should be based on what DSLs have been told about the content of the imagery.

The decision to view imagery should be based on the professional judgement of the DSL and should always comply with the child protection policy and procedures of the school or college. Imagery should never be viewed if the act of viewing will cause significant distress or harm to the pupil.

This Sexting advice has been produced on behalf of the UK Council for Child Internet Safety (UKCCIS) a group of more than 200 organisations from across government, industry, law, academia and charity sectors, working in partnership to help keep children safe online. The production of the advice has been co-ordinated by the UKCCIS Education Group, a partnership of the following organisations: Barnardo’s, The National Crime Agency’s CEOP Command, Childnet and Department for Education

PREVENT - Preventing Radicalisation And Extremism

All staff are expected to uphold and promote the fundamental principles of British values, including democracy, the rule of law, individual liberty and mutual respect, and tolerance of those with different faiths and beliefs. In formulating this policy, the Governors have taken account of the guidance from the Department for Education (DfE) who has called for all public bodies to make explicit their preventative measures to minimise the threat of extremism in their setting.

**DEFINITIONS AND INDICATORS**

Radicalisation is defined as the act or process of making a person more radical or favouring of extreme or fundamental changes in political, economic or social conditions, institutions or habits of the mind.

Extremism is defined as the holding of extreme political or religious views. The Governing Body has a zero tolerance approach to extremist behaviour for all community members. We rely on our strong values to steer our work

and ensure the pastoral care of our pupils protects them from exposure to negative influences. Furthermore, our positive promotion of our Code of Conduct, “Be Kind: Be Safe: Be Responsible,” equips our pupils with the skills to

reject violence in all its forms.

**AIMS AND PRINCIPLES**

The main aims of this policy statement are to ensure that staff are fully engaged in being vigilant about radicalisation; that they overcome professional disbelief that such issues will not happen here and ensure that we work alongside other professional bodies and agencies to ensure that our pupils are

safe from harm.

The principle objectives are that:

• Pupils are encouraged to adopt and live out our Core Values. These complement the key “British Values” of tolerance, respect, understanding, compassion and harmonious living.

• Pupils are helped to understand the importance of democracy and freedom of speech, through the SEAL (Social,emotional.aspects of learning) assemblies and through the elected School Council members

• Pupils are taught how to keep themselves safe, in school and when using the internet.

Pupils participate in local community events so that they appreciate and value their neighbours and friends who may not share their faith background.

• Pupil’s wellbeing, confidence and resilience is promoted through our planned curriculum and out of hours learning opportunities. • Pupils are supported in making good choices from a very young age, so

they understand the impact and consequences of their actions on others.

Governors, teachers, teaching assistants and non‐teaching staff demonstrate an understanding of what radicalisation and extremism are and why we need to be vigilant in school.

The Office for Security & Counter Terrorism works to counter the threat from terrorism and their work is detailed in the counter terrorism strategy CONTEST.

This strategy is based on four areas of work:

• Pursue - To stop terrorist attacks

• Prevent - To stop people becoming terrorists or supporting terrorism

• Protect - To strengthen our protection against a terrorist attack

• Prepare - To mitigate the impact of a terrorist attack

Our role, as a school, is outlined more specifically in the DCSF document

‘Learning together to be safe: A toolkit to help schools contribute to the prevention of violent extremism.’ Primarily our work will be concerned with PREVENTION and is outlined more specifically in the DCSF document ‘Learning together to be safe: A toolkit to help schools contribute to the prevention of violent extremism.’

This policy should be read alongside the school’s Safeguarding, Equal Opportunities, E‐Safety and Anti‐bullying policies.

Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be   
downloaded from:

[http://www.swgfl.org.uk/Staying-Safe/Creating-an-Online Safety-policy](http://www.swgfl.org.uk/Staying-Safe/Creating-an-E-Safety-policy)

**Information and support**

There is a wealth of information available to support schools and colleges to keep children safe online. The following is not exhaustive but should provide a useful starting point:

www.thinkuknow.co.uk

www.disrespectnobody.co.uk

www.saferinternet.org.uk

www.internetmatters.org

www.childnet.com/cyberbullying-guidance

www.pshe-association.org.uk

educateagainsthate.com

www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

KCSIE 2015

KCSIE 2016

23

Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Safety Policy Template and of the 360 degree safe Online Safety Self Review Tool:

• Members of the SWGfL Online Safety Group

• Avon and Somerset Police

• Representatives of SW Local Authorities

• Plymouth University Online Safety

• NEN / Regional Broadband Grids

• Graham Lowe, LSCB Online Safeguarding Advisor. www.lancashiresafeguarding.org.uk/online-safeguarding

Copyright of these Template Policies is held by SWGfL. Schools / Academies and other educational institutions are permitted free use of the Template Policies for the purposes of policy review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL ([esafety@swgfl.org.uk](mailto:esafety@swgfl.org.uk)) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is

accurate, as at the date of publication in October 2013. However, SWGfL can not

guarantee it’s accuracy, nor can it accept liability in respect of the use of the material.

© SWGfL 2013

**Revision Date**

22nd May 2017 and incorporates KCSIE 15 and KCSIE 16 (KCSIE 15 and KCSIE 16 added 16th December 2016)

**APPENDIX A**

**Requirements for creating social media sites on behalf of Walton-le-Dale High School**

## **A.1 CREATION OF SITES**

## A.1.1 Staff members participating in social media for work purposes are expected to demonstrate the same high standards of behaviour as when using other media or giving public presentations on behalf of Walton-le-Dale High School.

## A.1.2 Prior to creating a site, careful consideration must be given to the purposes for using social media and whether the overall investment is likely to be worthwhile for achieving the proposed pedagogical outcome.

## A.1.3 The proposed audience and level of interactive engagement with the site, for example whether pupils, school staff or members of the public will be able to contribute content to the site, must be discussed with the school’s Headteacher.

## A.1.4 Staff members must consider how much time and effort they are willing to commit to the proposed site. They should be aware that maintaining a site is not a one-off task, but involves a considerable time commitment.

## A.1.5 The headteacher or relevant managers must take overall responsibility to ensure that enough resources are provided to keep the site refreshed and relevant. It is important that enough staff members are trained and are able to maintain and moderate a site in case of staff absences or turnover.

## A.1.6 There must be a careful exit strategy and a clear plan from the outset about how long the site will last. It must not be neglected, creating a potential risk to the school’s brand and image.

## A.1.7 Consideration must also be given to how the success of the site will be evaluated to assess whether the site has achieved the proposed objectives.

**A.2 CHILDREN AND YOUNG PEOPLE**

* + 1. When creating social media sites for children and young people and communicating with them using such sites, staff members must at all times be conscious of their responsibilities; staff must always act in the best interests of children and young people.
    2. When creating sites for children and young people, staff members must be alert to the risks to which young people can be exposed. Young people’s technical knowledge may far exceed their social skills and awareness – they may post sensitive personal information about themselves, treat online ‘friends’ as real friends, be targets for ‘grooming’ or become victims of cyberbullying.
    3. If children and young people disclose information or display behaviour or are exposed to information or behaviour on these sites that raises safeguarding or other concerns, appropriate authorities must be informed immediately. Failure to do so could expose vulnerable young people to risk of harm.
    4. Staff members must ensure that the sites they create or contribute to for work purposes conform to the *Good Practice Guidance for the Providers of Social* *Networking and Other User Interactive Services* (Home Office Task Force on Child Protection on the Internet, 2008)
    5. Staff members must also ensure that the webspace they create on third party sites comply with the site owner’s minimum age requirements (this is often set at 13 years). Staff members must also consider the ramifications and possibilities of children under the minimum age gaining access to the site.
    6. Care must be taken to ensure that content is suitable for the target age group and contributors or ‘friends’ to the site are vetted.
    7. Careful thought must be given to the profile of young people when considering creating sites for them. For example, the internet may not be the best medium to communicate with vulnerable young people (or indeed any age group) receiving confidential and sensitive services from the school or the County Council. It may not be possible to maintain confidentiality, particularly on third-party-hosted sites such as social networking sites, where privacy settings may not be strong enough to prevent breaches of confidentiality, however inadvertent. If in doubt, you must seek advice from your Communications Manager (or appropriate manager).

## **A.3 APPROVAL FOR CREATION OF OR PARTICIPATION IN WEBSPACE**

## A.3.1 Walton-le-Dale High School social media sites can be created only by or on behalf of the school. Site administrators and moderators must be Walton-le-Dale High School employees or other authorised people.

## A.3.2 Approval for creation of sites for work purposes, whether hosted by the school or hosted by a third party such as a social networking site, must be obtained from the headteacher.

## A.3.3 Approval for participating, on behalf of Walton-le-Dale High School, on sites created by third parties must be obtained from the the headteacher.

## A.3.4 Content contributed to own or third-party hosted sites must be discussed with and approved by the the headteacher.

## A.3.5 The headteacher must be consulted about the purpose of the proposed site and its content. In addition, the headteacher’s approval must be obtained for the use of the school logo and brand.

## A.3.6 Staff must complete the Social Media Site Creation Approval Form (Appendix B) and forward it to the headteacher before site creation.

A.3.7 Be aware that the content or site may attract media attention. All media enquiries must be forwarded to the headteacher immediately. Staff members must not communicate with the media without the advice or approval of the headteacher.

**A.4 CONTENT OF WEBSPACE**

A.4.1 Walton-le-Dale High School -hosted sites must have clearly expressed and publicised Terms of Use and House Rules. Third-party hosted sites used for work purposes must have Terms of Use and House Rules that conform to the school’s standards of professional conduct and service.

A.4.2 Staff members must not disclose information, make commitments or engage in activities on behalf of Walton-le-Dale High School without authorisation.

A.4.3 Information provided must be worthwhile and accurate; remember what is published on the site will reflect on the school’s image, reputation and services.

A.4.4 Stay within the law and be aware that child protection, privacy, data protection, libel, defamation, harassment and copyright law may apply to the content of social media.

A.4.5 Staff members must respect their audience and be sensitive in the tone of language used and when discussing topics that others may find controversial or objectionable.

A.4.6 Permission must be sought from the relevant people before citing or referencing their work or referencing service providers, partners or other agencies.

A.4.7 Walton-le-Dale High School-hosted sites must always include the school logo or brand to ensure transparency and confidence in the site. The logo should, where possible, link back to the relevant page on the school website.

A.4.8 Staff members participating in Walton-le-Dale High School-hosted or other approved sites must identify who they are. They must disclose their positions within the school on these sites.

A.4.9 Staff members must never give out their personal information such as home contact details or home email addresses on these sites.

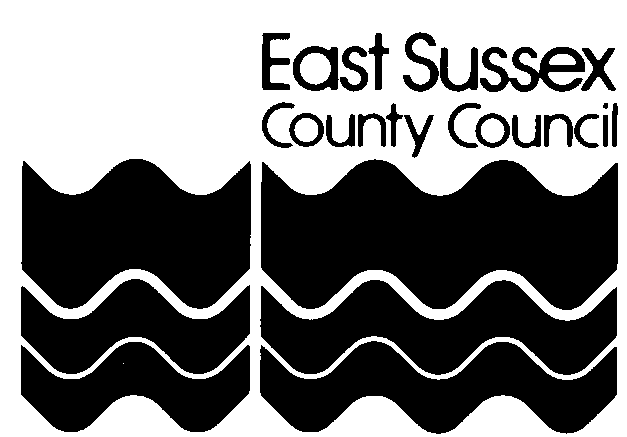
A.4.10 Personal opinions should not be expressed on official sites.

**A.5 CONTRIBUTORS AND MODERATION OF CONTENT**

* + 1. Careful consideration must be given to the level of engagement of contributors – for example whether users will be able to add their own text or comments or upload images.
    2. Sites created for and contributed to by pupils must have the strongest privacy settings to prevent breaches of confidentiality. Pupils and other participants in sites must not be able to be identified.
    3. The content and postings in Walton-le-Dale High School-hosted sites must be moderated. Moderation is the responsibility of the team that sets up or initiates the site.
    4. The team must designate at least two approved Administrators whose role it is to review and moderate the content, including not posting or removal of comments which breach the Terms of Use and House Rules. It is important that there are enough approved moderators to provide cover during leave and absences so that the site continues to be moderated.
    5. For third-party-hosted sites such as social networking sites used for work purposes, the responsibility for protection and intervention lies first with the host site itself. However, different sites may have different models of intervention and it is ultimately the responsibility of the staff member creating the site to plan for and implement additional intervention, for example in the case of content raising child safeguarding concerns or comments likely to cause offence.
    6. Behaviour likely to cause extreme offence, for example racist or homophobic insults, or likely to put a young person or adult at risk of harm must never be tolerated. Such comments must never be posted or removed immediately and appropriate authorities, for example the Police or Child Exploitation and Online Protection Centre (CEOP), informed in the case of illegal content or behaviour.
    7. Individuals wishing to be ‘friends’ on a site must be checked carefully before they are approved. Their comments must be reviewed regularly and any that do not comply with the House Rules must not be posted or removed.
    8. Any proposal to use social media to advertise for contributors to sites must be approved by the school’s headteacher.
    9. Approval must also be obtained from the school’s headteacherto make an external organisation a ‘friend’ of the site.

**APPENDIX B**

**Walton-le-Dale High School**

**Social Media Site Creation Approval Form**

**Use of social media on behalf of Walton-le-Dale High School must be approved prior to setting up sites.**

Please complete this form and forward it to the headteacher.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TEAM DETAILS** | | | | |
| Department |  | | | |
| Name of author of site |  | | | |
| Author’s line manager |  | | | |
| **PURPOSE OF SETTING UP SOCIAL MEDIA SITE**  **(please describe why you want to set up this site and the content of the site)** | | | | |
| What are the aims you propose to achieve by setting up this site?  What is the proposed content of the site? |  | | | |
| **PROPOSED AUDIENCE OF THE SITE**  **Please tick all that apply.** | | | | |
| ▢ Pupils of Walton-le-Dale High School  ▢ Walton-le-Dale High School staff  ▢ Pupils’ family members  ▢ Pupils from other schools (provide names of schools)  ▢ External organisations  ▢ Members of the public  ▢ Others; please provide details | | | | |
| **PROPOSED CONTRIBUTORS TO THE SITE**  **Please tick all that apply.** | | | | |
| ▢ Pupils of Walton-le-Dale High School  ▢ Insert school name staff  ▢ Pupils’ family members  ▢ Pupils from other schools (provide names of schools)  ▢ External organisations  ▢ Members of the public  ▢ Others; please provide details | | | | |
| **ADMINSTRATION OF THE SITE** | | | | |
| Names of administrators  (the site must have at least 2 approved administrators) | |  | | |
| Names of moderators  (the site must have at least 2 approved moderators) | |  | | |
| Who will vet external contributors? | |  | | |
| Who will host the site? | | ▢ Walton-le-Dale High School  ▢ Third party; please give host name | | |
| Proposed date of going live | |  | | |
| Proposed date for site closure | |  | | |
| How do you propose to advertise for external contributors? | |  | | |
| If contributors include children or adults with learning disabilities how do you propose to inform and obtain consent of parents or responsible adults? | |  | | |
| What security measures will you take to prevent unwanted or unsuitable individuals from contributing or becoming ‘friends’ of the site? | |  | | |
| **APPROVAL**  **(approval from relevant people must be obtained before the site can be created. The relevant managers must read this form and complete the information below before final approval can be given by the headteacher).** | | | | |
| **Line Manager**  **I approve the aims and content of the proposed site.** | | | Name |  |
| Signature |  |
| Date |  |
| **Headteacher** | | | Name |  |
| Signature |  |
| Date |  |