TITUS SALT SCHOOL

Cyber Security (E-safety) Policy

1.0 Introduction

Our Cyber Security policy recognises our commitment to e-safety and acknowledges its part in the school's overall safeguarding policies and procedures. It shows our commitment to meeting the requirements to keep pupils safe. It also ensures we meet all statutory requirements and takes account of Department of Education guidance. (See Appendix 1 for relevant extracts from 'Guidance for Safer Working Practice for Adults who work with Children and Young People')

We believe the whole school community can benefit from the opportunities provided by the internet and other technologies used in everyday life. The Cyber Security policy supports this by identifying the risks and the steps we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities. Our expectations for responsible and appropriate conduct are formalised in our Acceptable Use Policies (AUP) which we expect all staff and pupils to follow.

As part of our commitment to Cyber Security we also recognise our obligation to implement a range of security measures to protect the school network and facilities from attack, compromise and inappropriate use and to protect school data and other information assets. We have adopted the good practice requirements for all staff which are included in the Bradford Learning Network and e-safety mark documentation.

2.0 Our Commitment, Roles and Responsibilities

We believe that Cyber Security is the responsibility of the whole school community and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

The school will:

- Identify a person (the Cyber Security team) to take responsibility for Cyber Security and support them in their work
- Ensure adequate technical support is in place to maintain a secure ICT system
- Ensure policies and procedures are in place to ensure the integrity of the school's information and data assets
- Ensure effective liaison with the Governing Body
- Develop and promote a Cyber Security culture within the school community
- Ensure that all staff and pupils who access IT, within school or remotely, agree to the Acceptable Use Policy and that new staff have Cyber Security included as part of their induction procedure
- Make appropriate resources, training and support available to all members of the school community to ensure they are able to carry out their roles effectively with regard to Cyber Security

- Receive and regularly review Cyber Security incident logs and ensure that the correct procedures are followed should a Cyber Security incident occur in school and review incidents to see if further action is required
- Take ultimate responsibility for Cyber Security within the school community.

Staff will:

- Read, understand and help promote the school's Cyber Security policy and guidance
- Read, understand and adhere to the staff AUP
- Comply with the new Data Protection Act 2018 which includes the General Data Protection Regulation (EU) 2016/679 ("GDPR")
- Take responsibility for ensuring the safety of sensitive school data and information
- Develop and maintain an awareness of current Cyber Security issues and legislation and guidance relevant to their work
- Maintain a professional level of conduct in their personal use of technology at all times
- Embed Cyber Security messages in learning activities where appropriate
- Supervise pupils carefully when engaged in learning activities involving technology
- Ensure that pupils are told what to do should they encounter any material or receive communication which makes them feel uncomfortable
- Report all Cyber Security incidents which occur in the appropriate log and/or to their line manager
- Respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.

Additional responsibilities of ICT technical staff

- To support the school in providing a safe technical infrastructure to support learning and teaching
- To ensure appropriate technical steps are in place to safeguard the security of the school IT system, sensitive data and information. Review these regularly to ensure they are up to date.
- As part of BAU process or at the request of the Leadership team, conduct checks on files, folders, email and other digital content to ensure that the Acceptable Use Policy is being followed
- To report any Cyber Security related issues that come to their attention to the e-safety co-ordinator and/or Leadership team
- To ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems
- To ensure that suitable access arrangements are in place for any external users of the school's ICT equipment
- Liaise with the Local Authority and other agencies, e.g. West Yorkshire Police on e-safety issues.

Responsibilities of pupils

- To read, understand and adhere to the pupil Acceptable Use Policy and follow all safe practice guidance
- To take responsibility for their own and each other's safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school
- To respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home
- To understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- To report all Cyber Security incidents to appropriate members of staff
- To discuss Cyber Security issues in an open and honest way.

Responsibilities of parents and carers

- To help and support the school in promoting Cyber Security
- To read, understand and promote the pupil Acceptable Use Policy with their children
- To discuss Cyber Security concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology
- To consult with the school if they have any concerns about their children's use of technology.
- To keep up to date with current events and issues via the support on the school website

Responsibilities of Governing Body

- To read, understand, contribute to and help promote the school's Cyber Security policy and guidance as part of the school's overarching safeguarding procedures
- To support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents and carers to become engaged in Cyber Security awareness
- To ensure appropriate funding and resources are available for the school to implement the Cyber Security strategy.

Responsibilities of any external users of the school systems, e.g. adult or community education groups; breakfast or after-school clubs

- To take responsibility for liaising with the school on appropriate use of the school's ICT equipment and internet
- To ensure that participants follow the agreed Acceptable Use Policy.

Acceptable Use Policies (AUP)

Our Acceptable Use Policies are shared with all users yearly; staff and pupils will be expected to agree to follow their guidelines. We will ensure that external groups and

visitors who use our ICT facilities are made aware of the appropriate Acceptable Use Policy.

Currently the school has Acceptable Use Policy documents for:
- Pupils
- Staff.

3.0 Teaching and Learning

We believe that the key to developing safe and responsible behaviours online for everyone within our school community lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well and we have a duty to help prepare our pupils to benefit safely from the opportunities that these present. Learning how to use the internet and other technologies safely and responsibly also supports an understanding and appreciation of British values, including an appreciation that our use of the internet and other technologies is governed by the rule of law that protects individual citizens and is essential for their wellbeing and safety.

We will deliver a planned and progressive scheme of work to teach Cyber Security knowledge and understanding and to ensure that pupils have a growing understanding of how to manage the risks involved in online activity.

We believe that learning about Cyber Security should be embedded across the curriculum and also taught in specific lessons in Computing and PSHE. We will discuss, remind or raise relevant Cyber Security messages with pupils routinely wherever suitable opportunities arise through lessons, form time and assemblies; making the most of our own technology to embed this.

We will use our Digital Leaders, who are Childnet accredited, to deliver key messages to all pupils regarding Cyber Security. They will use a range of platforms to deliver key messages and run events that promote Cyber Security within the school and the wider community.

We will remind pupils about their responsibilities to which they have agreed through the Acceptable Use Policy. Staff and pupils will be reminded that third party content should always be appropriately attributed so as not to breach copyright laws.

Underpinning staff and pupil use of the internet and other technologies are the British values of:

- Tolerance and harmony
- Respect for other people
- Respect for democracy and support for participation in the democratic process.

How parents and carers will be involved
We believe it is important to help all our parents and carers develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will offer opportunities for finding out more information through meetings, e.g. the Parents' Information and Discussion Group, school publications, website and social networks.

We will ask all parents and carers to discuss the pupil Acceptable Use Policy with their children and to return a signed copy to school. We request our parents and carers support the school in applying the e-safety policy.

4.0 Managing and Safeguarding ICT Systems

The school will ensure that access to the school ICT system is as safe and secure as possible

Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software will be kept updated as appropriate. A firewall will be maintained and virus and malware protection installed on all appropriate hardware and kept active and up-to-date. Staff will have virus protection installed on all laptops used for school activity.

Any administrator or master passwords for school ICT systems will be kept secure and available to only those who require them.

The wireless networks available in school are protected by a range of security measures which prevent unauthorised access. New users can only be provided with access to wireless networks named individuals following a formal access process, e.g. the school's ICT technical staff. We will not allow anyone except ICT technical staff to download and install software onto the network.

Filtering internet access
The school employs multi-level content filtering to protect pupils from accessing inappropriate internet content. The first level of filtering is provided by the Local Authority working in partnership with Virgin Media. A second level of filtering is applied at school level and adds further rigour.

A dedicated firewall and content filtering hardware device is located in school and is the only route for external internet traffic (both incoming and outgoing). The device is maintained by the school's onsite ICT technical staff who respond immediately to alerts and requests for blocking and unblocking of content at a local level. A daily safeguarding report is generated and automatically emailed to appropriate members of staff for review of any logged incidents and to take further action when required.

Teachers are encouraged to check websites they wish to use. All users are informed about the action they should take if inappropriate material is accessed or discovered on a computer.

Access
The school decides which users should and should not have internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Effective arrangements are in place for visitors to the school who may be granted a temporary log in. All users are provided with a log in appropriate to their key stage or role in school. Pupils will learn about safe practice in the use of their log in and passwords during Computing lessons.

Staff will be given effective guidance on managing access to laptops which are used both at home and school and in creating secure passwords. Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information. Remote access is never allowed to unauthorised third party users.

5.0 Using the Internet

We provide the internet to:
- Support curriculum development in all subjects
- Support the professional work of staff as an essential professional tool
- Enhance the school's management information and business administration systems
- Enable electronic communication and the exchange of curriculum and administration data with the Local Authority, examination boards and others.

Users will be made aware that they must take responsibility for their use of, and their behaviour whilst using, the school ICT systems or a school-provided laptop or device and that such activity can be monitored and checked. All users of the school's ICT or electronic equipment will be expected to abide by the relevant Acceptable Use Policy at all times, whether working in a supervised activity or working independently.

Pupils and staff are informed about the actions to take if inappropriate material is discovered.

Email
Email is regarded as an essential means of communication and the school provides all members of the school community with an email account for school-based

communication. Email communication between staff, pupils and parents and carers will only be made using the school email account and should be professional and related to school matters only.

Email messages on school matters should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained. There are systems in place for storing relevant electronic communications which take place between school and parents and carers. Use of the school email system is monitored and checked.

As part of the curriculum, pupils are taught about safe and appropriate use of email. This takes place from the very first term in year 7 when all pupils are taught how to use the school email account professionally. Pupils are informed that misuse of email can result in a loss of privileges.

School website and social media

The school maintains editorial responsibility for any school initiated website, learning platform or social media channel content, e.g. YouTube, Twitter to ensure that content is accurate and the quality of presentation is maintained. The school maintains the integrity of the school website, learning platforms or social media by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the website is the school address, email and telephone number. Published contact details for staff are school provided. Identities of pupils are protected at all times. The school obtains permission from parents and carers for the use of pupils' photographs, images and other data in line with Data Protection Act 2018 and GDPR

Creating online content as part of the curriculum

As part of the curriculum we encourage pupils to create online style content which gives them an idea on guidelines for online content, without always the need to actually publish it. They are taught to publish for a wide range of audiences which might include governors, parents and carers or younger children. Blogging, podcasting and other publishing of online content by pupils will take place within the school learning platform or other media selected by the school. Pupils will only be allowed to post or create content on sites where members of the public have access, when this is part of a school related activity. Appropriate procedures to protect the identity of pupils will be followed.

We take all steps to ensure that any material published online is the author's own work, gives credit to any other work included and does not break copyright.

Online material published outside the school

Staff and pupils are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school as they are in school.

Material published in a social context by pupils and/or staff which is considered to bring the school into disrepute or is considered to be harmful to, or harassment of another pupil or member of staff will be considered a breach of school discipline and treated accordingly.

6.0 Using Images, Video and Sound

We recognise that many aspects of the curriculum can be enhanced by the use of multi-media and that there are a wide and growing range of devices on which this can be accomplished. Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound. They are taught how to search for royalty free media which does not infringe on Copyright.

Digital images, video and sound recordings are only taken with the permission of participants; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

The school obtains permission from parents and carers for the use of pupils' photographs, images in videos and other data in line with Data Protection Act 2018 and GDPR. This permission is checked whenever an activity is photographed or filmed.

7.0 Using Mobile Phones/Tablets

Unauthorised or secret use of a mobile phone or other electronic device, to record voice, pictures or video is forbidden. Unauthorised publishing of such material on a website which causes distress to the person(s) concerned will be considered a breach of school discipline, whether intentional or unintentional. The person responsible for the material will be expected to remove this immediately upon request.

Using other technologies

We will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from a Cyber Security point of view. We will regularly review the Cyber Security policy to reflect any new technology that we use, or to reflect the use of new technology by pupils.

Staff or pupils using a technology not specifically mentioned in this policy will be expected to behave with similar standards of behaviour to those outlined in this document.

8.0 Protecting School Data and Information

We recognise our obligation to safeguard staff and pupils' personal data including that which is stored and transmitted electronically. We regularly review our practices and procedures to ensure that we meet this basic obligation.

The school is a registered Data Controller under the Data Protection Act 2018 and we will comply at all times with the requirements of that registration.

Pupils are taught about the need to protect their own personal data as part of their Cyber Security awareness and the risks resulting from giving this away to third parties.

Suitable procedures and where necessary, training are in place to ensure the security of such data including the following:

- When data is copied onto a CD it is encrypted/password protected so that in the event of loss/misplacement data is not compromised
- All computers or laptops holding sensitive information are set up with strong passwords; staff are required to password protect screen savers and lock screens when they are left unattended.
- Staff are provided with appropriate levels of access to the school's management information system holding pupil data. Passwords are not shared and administrator passwords are kept securely
- Staff are aware of their obligation to keep sensitive data secure when working on computers outside school
- Staff are advised that when they access the school network remotely from a personal computer it is regularly updated with the latest security patches and has anti-virus software installed
- When we dispose of old computers and other equipment we take due regard for destroying information which may be held on them
- We follow Local Authority procedures for transmitting data securely and sensitive data is not sent via email unless encrypted
- Remote access to computers is by authorised personnel only
- We have full back-up and recovery procedures in place for school data.

9.0 Dealing with Cyber Security Incidents

All Cyber Security incidents are recorded in the school Cyber Security Log which is regularly reviewed. Any incidents where pupils do not follow the Acceptable Use Policy will be dealt with following the school's normal behaviour or disciplinary procedures.

In situations where a member of staff is made aware of a serious Cyber Security incident, concerning pupils or staff, they will inform the Cyber Security co-ordinator/Year Team, their line manager or Headteacher who will then respond in the most appropriate manner.

Instances of cyber bullying will be taken very seriously by the school and dealt with using the school's anti-bullying procedures. School recognises that staff as well as pupils may be victims and will take appropriate action in either situation.

Incidents which create a risk to the security of the school network, or create an information security risk, will be referred to the school's Cyber Security co-ordinator and ICT technical staff and appropriate advice sought and action taken to minimise the risk and prevent further instances occurring; including reviewing any policies, procedures or guidance. If the action breaches school policy then appropriate sanctions will be applied. The school will decide if parents and carers need to be informed if there is a risk that pupil data has been lost.

School reserves the right to monitor and search any technology equipment on the premises, including personal equipment, including when a breach of this policy is suspected.

Dealing with complaints and breaches of conduct by pupils

- Any complaints or breaches of conduct will be dealt with promptly
- Responsibility for handling serious incidents will be given to a senior member of staff
- Parents and carers and the pupil will work in partnership with staff to resolve any issues arising
- There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies.

The following activities constitute behaviour which we would always consider unacceptable (and possible illegal):

- Accessing inappropriate or illegal content deliberately
- Deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Continuing to send or post material regarded as harassment, or of a bullying nature after being warned
- Using digital communications to communicate with pupils in an inappropriate manner, e.g. using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites.

The following activities are likely to result in disciplinary action:

- Accessing inappropriate or illegal content accidentally and failing to report this
- Inappropriate use of personal technologies, e.g. mobile phones, at school or in lessons
- Sharing files which are not legitimately obtained, e.g. music files from a file sharing site
- Using school or personal equipment to send a message, or create content, that is offensive or bullying in nature or could bring the school into disrepute
- Attempting to circumvent school filtering, monitoring or other security systems

- Circulation of commercial, advertising or 'chain' emails or messages
- Revealing the personal information, including digital images, videos and text, of others by electronic means, e.g. sending of messages, creating online content, without permission
- Using online content in such a way as to infringe copyright or failing to acknowledge ownership, including plagiarising of online content
- Transferring sensitive data insecurely or infringing the conditions of the Data Protection Act, revised 1988.

The following activities would normally be unacceptable however, in some circumstances they may be allowed, e.g. as part of planned curriculum activity or as system administrator to problem solve

- Accessing non-educational websites, e.g. gaming or shopping websites during lesson time.

10.0 Dealing with a Child Protection Issue Arising from the Use of Technology

If an incident occurs which raises concerns about Child Protection or the discovery of indecent images on the computer, then the procedure outlined in the school's Safeguarding Policy will be followed.

11.0 Policy and Review

The effectiveness of the policy is monitored by those members of the Senior Leadership Team who take responsibility for co-ordinating its implementation. The Policy will be reviewed annually or more often if events indicate this is appropriate.

Appendix 1

Extract from: Guidance for Safer Working Practice for Adults who work with Children and Young People. DCSF January 2009

Section 12 Communication with Children and Young People (including the Use of Technology)

Communication between children and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny.

Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. E-mail or text communications between an adult and a child young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites.

Internal e-mail systems should only be used in accordance with the organisation's policy.

This means that the organisation should:

- have a communication policy which specifies acceptable and permissible modes of communication

This means that adults should:

- not give their personal contact details to children or young people, including their mobile telephone number and details of any blogs or personal websites
- only use equipment e.g. mobile phones, provided by organisation to communicate with children, making sure that parents have given permission for this form of communication to be used
- only make contact with children for professional reasons and in accordance with any organisation policy
- recognise that text messaging is rarely an appropriate response to a child in a crisis situation or at risk of harm. It should only be used as a last resort when other forms of communication are not possible
- not use internet or web-based communication channels to send personal messages to a child/young person

- ensure that if a social networking site is used, details are not shared with children and young people and privacy settings are set at maximum

Section 27 Photography and Videos

Working with children and young people may involve the taking or recording of images. Any such work should take place with due regard to the law and the need to safeguard the privacy, dignity, safety and well-being of children and young people. Informed written consent from parents or carers and agreement, where possible, from the child or young person, should always be sought before an image is taken for any purpose.

Careful consideration should be given as to how activities involving the taking of images are organised and undertaken. Care should be taken to ensure that all parties understand the implications of the image being taken especially if it is to be used for any publicity purposes or published in the media, or on the Internet. There also needs to be an agreement as to whether the images will be destroyed or retained for further use, where these will be stored and who will have access to them.

Adults need to remain sensitive to any children who appear uncomfortable, for whatever reason, and should recognise the potential for such activities to raise concerns or lead to misunderstandings.

It is not appropriate for adults to take photographs of children for their personal use. This means that adults should:

- be clear about the purpose of the activity and about what will happen to the images when the activity is concluded
- be able to justify images of children in their possession
- avoid making images in one to one situations or which show a single child with no surrounding context
- Ensure the child/young person understands why the images are being taken and has agreed to the activity and that they are appropriately dressed.
- only use equipment provided or authorised by the organisation
- report any concerns about any inappropriate or intrusive photographs found
- always ensure they have parental permission to take and/or display photographs

This means that adults should not:

- display or distribute images of children unless they have consent to do so from parents/carers
- use images which may cause distress
- use mobile telephones to take images of children
- take images 'in secret', or taking images in situations that may be construed as being secretive.

Section 28 Access to Inappropriate Images and Internet Usage

There are no circumstances that will justify adults possessing indecent images of children. Adults who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children on the internet is illegal. This will lead to criminal investigation and the individual being barred from working with children and young people, if proven.

Adults should not use equipment belonging to their organisation to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.

Adults should ensure that children and young people are not exposed to any inappropriate images or web links. Organisation's and adults need to ensure that internet equipment used by children have the appropriate controls with regards to access. E.g. personal passwords should be kept confidential.

Where indecent images of children or other unsuitable material are found, the police and Local Authority Designated Officer (LADO) should be immediately informed. Adults should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.

This means that organisation's should
- have clear e-safety policies in place about access to and use of the internet
- Make guidance available to both adults and children and young people about appropriate usage.

This means that adults should:
- follow their organisation's guidance on the use of IT equipment
- ensure that children are not exposed to unsuitable material on the internet
- ensure that any films or material shown to children and young people are age appropriate