GREENWOOD ACADEMIES TRUST

E-Safety Procedure

Version: 7.0 Approval Status: Approved

Document Owner:	Graham Feek
Classification:	External
Review Date:	21/06/2021
Reviewed:	25/05/2018

Table of Contents

1. The Purpose of this Procedure Document

The Greenwood Academies Trust E-Safety Policy sets out the overall policy context in which the Trust will manage e-safety within its academies. This Procedure Document sets out in more detail

the underlying responsibilities and processes to ensure the overall aims of the Policy are delivered.

2. Roles and Responsibilities

The Trust Board

The Trust Board is responsible for reviewing the overall effectiveness of the policy. This will be carried out by the Trust Board receiving regular information about e-safety incidents and monitoring reports. A member of the Trust Board has the role of Safeguarding Champion, which includes E-Safety.

The Principal and Senior Leaders

- The Principal has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator (ESC). Because of the close relationship between E-safety and Safeguarding, the Designated Safeguarding Lead (DSL) will often also be the ESC.
- The Principal, the Senior Leadership Team and the ESC should be aware of the procedures to be followed in the event of a safeguarding allegation, including those relating to E-safety, being made against a member of staff. These procedures are included in the Trust's Safeguarding Policy and Managing Allegations against Staff Procedure.
- The Principal is responsible for ensuring that the ESC and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Principal will ensure that there is a system in place to allow for monitoring and support of those in the academy who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the ESC.

E-Safety Co-ordinator (ESC)

The ESC:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety procedures.
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with IT Service Lead through service review meetings.
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- reports regularly to Senior Leadership Team

The E-safety Co-ordinator should be trained in e-safety issues and be aware of the potential for serious child protection and 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

The E-safety Co-ordinator may often be the Designated Safeguarding Lead (DSL) because of

the close link between e-safety and safeguarding.

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current academy e-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 Principal for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Trust's Digital Citizenship Contract (DCC)
- pupils 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, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

DSL Group

The DSL Group provides a consultative group that has wide representation from the Academy community, with responsibility for safeguarding which includes e-safety and the monitoring of the E-safety Policy, including the impact of initiatives.

Members of the DSL Group will assist with:

- the production / review / monitoring of the school e-safety policy / documents.
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- consulting stakeholders – including parents / carers and the pupils about the e-safety provision.

Pupils:

- are responsible for using the Academy digital technology systems in accordance with their DCC
- 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 e-safety practice when using digital technologies out of school and realise that the Academy's E-Safety Policy covers their actions out of school, if related to their membership of the Academy.

Parents and Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The Academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national and local e-safety campaigns and literature. Parents and carers

will be encouraged to support the Academy in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at Academy events
- access to parents' sections of the website
- their children's personal devices in the Academy (where this is allowed).

Community Users

Community Users who access Academy systems/website as part of the wider Academy provision will be expected to sign a Community User AUP before being provided with access to Academy systems. (A Community Users Acceptable Use Agreement Template can be found in the appendices).

IT Directorate

The IT Directorate is responsible for ensuring:

- that the Academy's technical infrastructure is secure and is not open to misuse or malicious attack
- that the Academy meets required e-safety technical requirements as directed by the Trust's IT Director
- 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 through appropriate vendor solutions and is updated on a regular basis, in consultation with the Academy Principal.
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal for investigation / action / sanction
- that monitoring software / systems are implemented based on Central IT policy.
- monitoring network / internet / incident logs.

3. Policy Statements

3.1 Education – Pupils

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

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

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the pupil DCC 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 pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, the Principal can request via the Director of IT or the IT Service Desk to 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.

3.2 Education – Parents and Carers

Many parents and carers have only a limited understanding of e-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 Academy will therefore seek to provide information and awareness to parents and carers through:

- curriculum activities
- letters, newsletters, websites
- parents / carers' evenings / sessions
- high profile events / campaigns eg Safer Internet Day
- reference to the relevant web sites / publications eg www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers
  (see appendix for further links / resources)

3.3 Education and Training – Staff and Volunteers

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

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policy.
- The ESC will receive regular updates through attendance at external training events by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The ESC will provide advice / guidance / training to individuals as required.

The Safeguarding Training Curriculum will include relevant e-safety training.

3.4 Training – Trustees and Academy Advisory Council Members

Trustees and Academy Advisory Council Members should take part in e-safety awareness sessions. This may be offered in a number of ways and will be set out the Safeguarding Training Curriculum:

- Attendance at training provided by the various organisations.

- Participation in Academy training / information sessions for staff or parents

4. Technical – infrastructure, equipment, filtering and monitoring

The IT Directorate will be responsible for ensuring that the Academy 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 E-safety responsibilities.

The IT Directorate will ensure that:

- Academy technical systems will be managed in ways that ensure that the Academy meets recommended technical requirements
- there will be regular reviews and audits of the safety and security of 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 Academy technical systems and devices.
- it 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
- Internet access is filtered for all users. Illegal or inappropriate content is filtered by the broadband or filtering provider by actively employing appropriate content filtering. Content lists are regularly updated and internet use is logged and regularly monitored.
- the process is followed to deal with requests for filtering changes
- regular monitoring and recording of the activity of users on the Academy technical systems and users are made aware of this in the AUP.
- an appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- that 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 Academy 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” (eg trainee teachers, supply teachers, visitors) onto the Academy systems.
- an agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on Academy devices that may be used out of school.
- an agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on Academy devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on Academy devices.
- Personal data cannot be sent over the internet, taken off the Academy site or transferred by any other means (physical or electronically) unless there is express written consent to do so from the Principal and IT Director. Obtaining Data sharing agreements and ICO certification may be necessary before this approval is granted. Only then can the transfer of personal data take place using a Trust approved method. You should always seek advice on this matter from the Principal or IT Service Desk.

5. Bring Your Own Device (BYOD)

The Trust’s position in relation to BYOD is determined academy by academy. There are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy, which are covered in the DCC.

6. Use of Biometric Information

The Protection of Freedoms Act 2012 includes measures that will affect schools and colleges that use biometric recognition systems, such as fingerprint identification and facial scanning:

- For all pupils in schools and colleges under 18, they must obtain the written consent of a parent before they take and process their child's biometric data.
- They must treat the data with appropriate care and must comply with data protection principles as set out in the General Data Protection Regulation (GDPR) 2018.
- They must provide alternative means for accessing services where a parent or pupil has refused consent.
- Any proposed biometric system must be approved by the Chief Executive.

7. Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber bullying 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 Academy 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 pupils 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 and carers are welcome to take videos and digital images of their children at Academy events for their own personal use (as such use is not covered by the GDPR). 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 and carers comment on any activities involving other students in the digital and video images.
- Staff and volunteers are allowed to take digital and video images to support educational aims, but must follow Academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Academy equipment, the personal equipment of staff should not be used for such purposes. Copyright of all photographs or videos belong to the Trust and any reproduction or distribution of the photographs or videos by a third party will constitute an infringement of copyright without the written permission of the Trust and must be accompanied by a credit or by-line stating the authorship of the photographs or videos.
- Care should be taken when taking digital and video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the Academy into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs or videos will not be substantially edited, adapted or altered from their original intention or purpose, or used for anything which may be viewed as negative in tone or that may cause offence, embarrassment or distress. The full names (first name and surname) of pupils will not be disclosed without good reason. For example, we may include the full name of a pupil if they have won an award. Pupil addresses will not be disclosed in detail, but we may state, for example, 'Sally from Skegness'.
- Written permission from parents or carers will be obtained before photographs and videos of pupils are taken. Where a pupil reaches the age of 13, written consent will also be sought from them.

8. Data Protection

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

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept no longer than is necessary
- Processed in a manner that ensures appropriate security

The specific requirements for academies are set out in the Trust's Data Protection Policy.

Staff must ensure that they follow the requirements set out in the staff AUP in relation to the storage and transfer of data, including:

- at all times taking care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- using 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
- transferring data using encryption and secure password protected devices.

9. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

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

- The official Academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the Academy 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 and carers (email, chat,) must be professional in tone and content. These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or social media must not be used for these communications.

- Whole class / group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual Academy email addresses for educational use. (academies may choose to use group or class email addresses for younger age groups eg. at KS1.)
- Pupils should be taught about e-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 Academy website and only official email addresses should be used to identify members of staff.

10. Social Media - Protecting Professional Identity

The Staff AUP and Student DCC set out the expectations about the appropriate use of social media by staff, pupils and parents/carers. This guidance must be followed in order to ensure

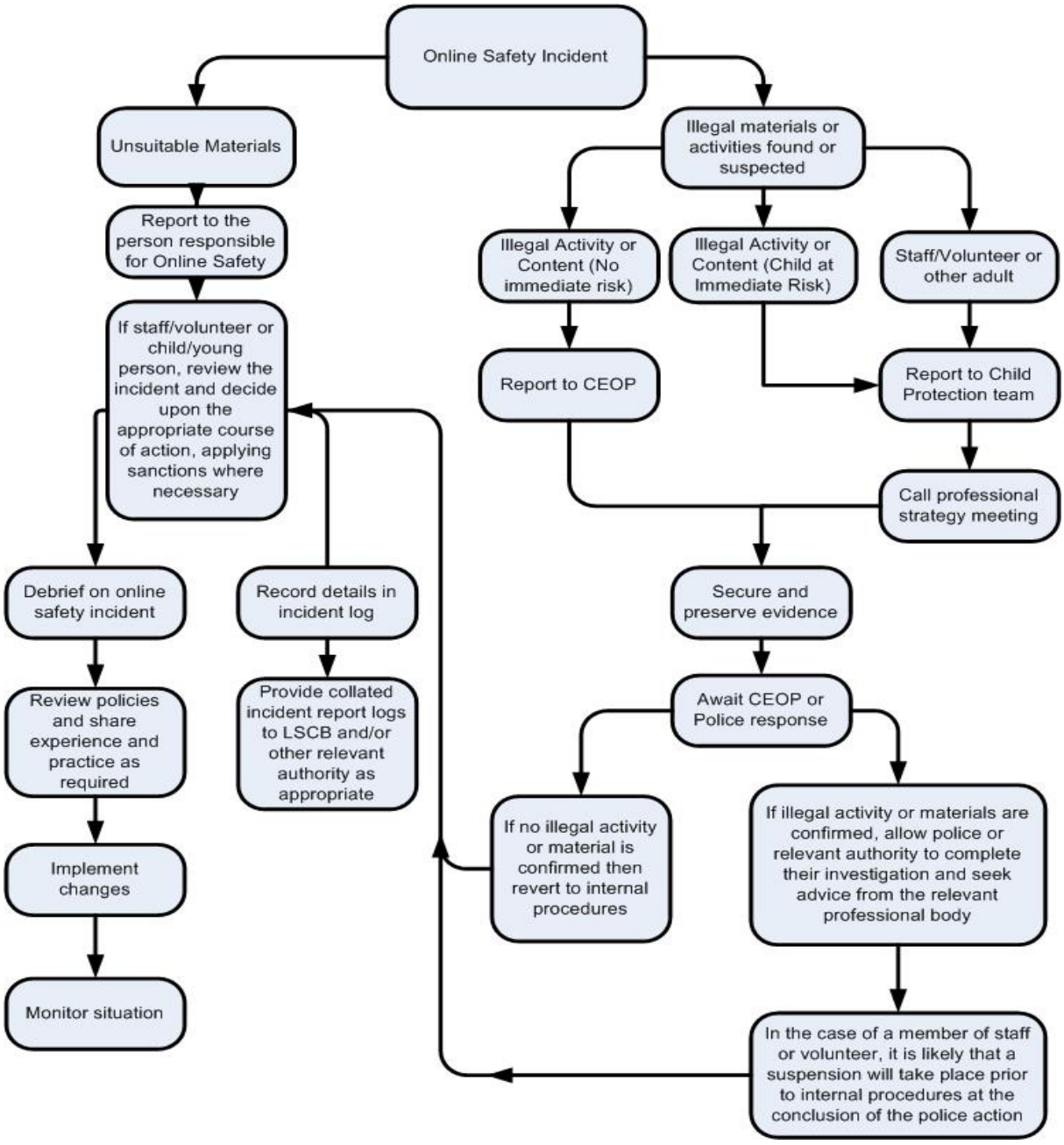
that staff, pupils and parents/carers do not engage in activity which may cause them to breach acceptable standards of conduct.

11. Unsuitable / inappropriate activities
Responding to incidents of misuse

The staff AUP and Student DCC set out the requirements in relation to reporting unsuitable or inappropriate activities. Where such activities also raise a safeguarding concern, the Trust's Safeguarding Policy and relevant procedures must be followed.

12. Illegal Incidents

If there is a suspicion that a safeguarding issue has taken place then the DSL will make a referral based on the flowchart below.



* Please note that reporting to 'Child Protection Team' should be undertaken as set out within the Trust's Safeguarding Policy and will normally be referred by the Principal or Designated Safeguarding Lead.

13. Securing Evidence and Preserving Evidence

Evidence should only be viewed and evidence stored by the DSL. They should use a designated PC. The PC should be in a secure office, not over looked by others, and made available to the DSL only for the duration of the investigation or prosecution.

If it is necessary to store child protection information on portable media, such as a CD or flash drive, these items should also be kept in locked storage. The locked storage should be controlled by the Principal/DSL.

Child protection records are normally exempt from the disclosure provisions of the GDPR, which means that children and parents do not have an automatic right to see them. If any member of staff receives a request from a child or parent to see child protection records, they should refer the request to the Principal.
To facilitate secure storage of evidence:

- A 'DSL' folder will be created on the main academy file server, outside of the current 'shared file' structure.
- The DSL folder will have auditing enabled on all contents. Audit will be set for all Read and Write activities.
- Folder permissions set to the DSL and Principal only.
- IT staff can aid the DSL to move files to the folder. They must be supervised during this operation by the DSL or Principal.
- DSL updates school file with location of files.
- DSL will review data periodically to ensure it is deleted when no longer required. (Secure deletion to be reviewed).
- DSL will delete files that are no longer required as per the review.

14. Other Incidents

It is hoped that all members of the Academy community will be responsible users of digital technologies, who understand and follow Academy 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:

- The Academy Principal will ensure that more than one senior member of staff involved in this process, which will include a nomination by the IT Director. 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 used for investigation (see the 'Serious Misconduct' Procedure below). 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 Academy 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.

SERIOUS MISCONDUCT

Where serious misconduct or an incident has taken place and evidence exists in electronic format, the data may be stored for use at a later date. The responsibility of managing this data from a data protection aspect is that of the Principal.

To facilitate secure storage of evidence:

- A 'MISCONDUCT' folder will be created on the main academy file server, outside of the current 'shared file' structure.
- The DSL folder will have auditing enabled on all contents. This will be for all Read and Write activities.
- Folder permissions set to DSL and Principal only. Further staff may be added by request to the service desk.
- IT staff may transfer files from other devices/Internet/email to the folder.
- SDL updates register contained in the 'MISCONDUCT' folder with details of the file.
- IT staff to remove the files when no longer required

The following questions are pertinent when considering the retention of files in the 'MISCONDUCT' folder. This folder falls under the normal rules for data protection purposes.

- Is the person identifiable from the data being stored?
- How long does the data need to be kept for?
- Who has access to the data?
- Who controls the data?
- Will the data be shared with any third parties? Will this be given to the Police or Social Services?
- Is the reason for recording the data clearly defined? Is it absolutely necessary to retain the data for the purposes of the follow-up/investigation? For example, do we need a video of two pupils fighting if a number of witnesses have already testified to the event?
- Is the person identified in the data consenting to the data being shared? For example, pupils standing in the background.

15. Academy Actions and Sanctions

It is more likely that the Academy 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 Academy community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour and disciplinary procedures.

16. Appendices

Appendix 1 Guidance on the Digital Citizenship contract

Appendix 2 Fair Processing Notice – Images (photos and films)

Appendix 3 Use of Cloud services

Appendix 4 Record of reviewing sites (for internet misuse)

Appendix 5 Academy Reporting Log template

Appendix 6 Academy E-Safety Training Needs Audit template

Appendix 7 Information to parents/careers – the “Privacy Notice”

Appendix 8 Risk Assessment

Appendix 9 Search Policy

Appendix 10 Search Policy statement

Appendix 11 Legislation

Appendix 12 Filtering Policy

Appendix 13 Links to other organisations and documents

Appendix 14 Glossary of terms

Appendix 1

GREENWOOD DALE FOUNDATION TRUST

Guidance on the Digital Citizen Contract

Pupils in Key Stage 1 – There should be an expectation that teachers will verbally share the contents of the **Digital Citizenship Contract KS2** with children – talking through and explaining the language. The document could be displayed in the classroom and ICT suite as a visual reference.

Pupils in Key Stage 2 – At KS2 an Academy may want the **Digital Citizenship Contract KS2** to go home as part of the home/Academy agreement that pupils and parents/carers sign. If it is not signed it should still be shared and displayed somewhere appropriate and form part of the staying safe and IT curriculum.

Pupils in Key Stage 3-5 – At KS3-5 the **Digital Citizenship Contract KS3-5** should be used. This requires that pupils and parents sign up to the document and a signing page is provided on Page 5 to be returned and retained by the Academy. The rest of the document should be retained by the parent/carer for reference as it contains useful information and resources to help protect their children online.

Appendix 2

GREENWOOD ACADEMIES TRUST

Further information

Fair Processing Notice - Images (photos and films)

- The full names (first name and surname) of pupils will not be disclosed without good reason. For example, we may include the full name of a pupil if they have won an award. Pupil addresses will not be disclosed in detail, but we may state, for example, 'Sally from Skegness' **.
- The photographs or videos will not be substantially edited, adapted or altered from their original intention or purpose, or used for anything which may be viewed as negative in tone or that may cause offence, embarrassment or distress.
- Copyright of all photographs or videos belong to the Greenwood Academies Trust (GAT).
- Any reproduction or distribution of the photographs or videos by a third party will constitute an infringement of copyright without the written permission of the GAT and must be accompanied by a credit or by-line stating the authorship of the photographs or videos.
- Photographs or films may be used after your child leaves the Academy without consent as long as it is for their original purpose. It is expected that these will be deleted after a reasonable period of time.
- We may use photo and films on websites and social media which can be viewed throughout the world and not just in the United Kingdom where UK law applies.
- We may supply photos and films to the local, regional or national media for use in newspapers, in magazines or on TV. The media are exempt from the GDPR and may want to include the full details for pupils they photograph or film including full name, age and where they live.

Appendix 3

GREENWOOD ACADEMIES TRUST

Use of Cloud-based Services

Before committing to an agreement to use a cloud system there are a number of checks that should be made on behalf of the Academy.

The Central IT service will need to assess the following:

- Third Party Sharing Agreement
- ICO Registration
- Member of Safe Harbour registration

The principal should contact the Regional Service Delivery Lead when investigating the use of any “Cloud Systems” before entering in to an agreement with a vendor.

Appendix 4

GREENWOOD ACADEMIES TRUST

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Website(s) address / device **Reason for concern**

Conclusion and Action proposed or taken

Appendix 5

Academy Reporting Log Template

Reporting Log

Group .....

Date	Time	Incident	Action taken		Incident Reported by	Signature
			What?	By whom?		

Appendix 6

E-Safety Training Needs Audit

Training Needs Audit Log

Group ..... Date .....

Name /Position	Relevant training in last 12 months	Identified training need	To be met by:	Cost	Review date

Appendix 7

GREENWOOD ACADEMIES TRUST

Information to Parents / Carers – the 'Privacy Notice'

In order to comply with the fair processing requirements of the DPA, the Academy will inform parents / carers of all pupils / students of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed.

This privacy notice will be passed to parents / carers through examples such as the website, Prospectus, newsletters, reports or a specific letter / communication. Parents / carers of young people who are new to the Academy will be made aware of the Privacy Notice through the above media.

** Please refer to the Privacy Policy for Pupils and Parents and for Staff.*

Appendix 8

GREENWOOD ACADEMIES TRUST

Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

Risk assessments are an on-going process and should result in the completion of an Information Risk Actions Form (example below):

Risk ID	Information Asset affected	Information Asset Owner	Protective Marking (Impact Level)	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

Appendix 9

GREENWOOD ACADEMIES TRUST

Electronic Devices - Searching and Deletion Policy

The Education Act 2012 sets out what the law is presumed to be, based on prior legal and educational knowledge, and common sense. Rights and responsibilities regarding physical contact and personal data are still evolving rapidly. So too are social, entertainment and educational technologies and the skills necessary to use them safely and prudently. This is particularly so where those who are under 18 are involved.

No existing law or policy can fully insulate anyone from the risk involved in searching for, access to or deletion of the personal data of others. Anyone refraining from any such search, access or deletion when hindsight shows circumstances merit such actions may however be at significant risk and may put seriously at risk the wellbeing of children entrusted to their care. This policy cannot therefore be relied on as justification for any act or lack of action by anyone – there is no substitute for the proper and well documented exercise of adequately informed professional judgement.

It is for each Academy's Principal to apply and monitor application of their own policies as guided by their Education Director. The Trust Board determines this policy.

Introduction

The changing face of information technologies and ever increasing pupil and student use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge, but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.

The particular changes we deal with here are the added power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.

Items banned under the academy rules (section 89 Education and Inspections Act 1996) are publicised in the Trust's Home to Academy Agreement. An item which is banned or whose use is banned by the academy rules may be searched for under these powers.

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the Academy rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The Principal must publicise the Academy's Behaviour Policy, in writing, to staff, parents / carers and pupils at least once a year.

DfE advice on these sections of the Education Act 2011 can be found in the document: 'Screening, searching and confiscation – Advice for head teachers, staff and governing bodies'.

http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

It is recommended that Principals (and, at the least, other senior leaders) should be familiar with this guidance.

Relevant legislation:

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 Part 2 (Discipline)
- The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990

This is not a full list of Acts involved in the formation of this advice. Further information about relevant legislation can be found via the above link to the DfE advice document.

Responsibilities

The Trust is responsible for ensuring that the Academy policies reflect the requirements contained within the relevant legislation. The Principal will need to authorise those staff who are allowed to carry out searches and who have undertaken appropriate training.

Training / Awareness

It is essential that all staff should be made aware of and should implement the Academy's policy.

Members of staff should be made aware of the Academy's policy on 'Electronic devices – searching and deletion':

- at induction
- at regular updating sessions on the Academy's e-safety policy

Members of staff authorised by the Principal to carry out searches for and of electronic devices and to access and delete data / files from those devices should receive training that is specific and relevant to this role. Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal. Please see guidance in main policy in relation to illegal incidents.

Appendix 10

GREENWOOD ACADEMIES TRUST

Search Policy Statement

The Academy Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

Pupils are allowed to bring mobile phones or other personal electronic devices to school and use them only within the rules laid down by the Academy within the Home/Academy Agreement.

If pupils breach these rules they will be subject to sanctions under the Academy's Behaviour Policy.

Authorised staff have the right to search for such electronic devices where they reasonably suspect that the data or files on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the Academy rules.

Searching with consent is where authorised staff may search with the pupil's consent for any item.

Searching without consent is where authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the Academy rules as an item which is banned and may be searched for.

The authorised member of staff must have reasonable grounds for conducting a search.

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search. (The powers included in the Education Act do not extend to devices owned (or mislaid) by other parties eg a visiting parent or contractor, only to devices in the possession of pupils.)

The authorised member of staff should take care that, where possible, searches should not take place in public places (eg an occupied classroom), which might be considered as exploiting the pupil being searched.

The authorised member of staff carrying out the search must be the same gender as the pupil being searched and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the pupil being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a pupil of the opposite gender, including without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

Use of Force cannot be used to search.

'Possessions' means any goods over which the pupil has or appears to have control – this includes desks, lockers and bags.

A pupil's possessions can only be searched in the presence of the pupil and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

Electronic Devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the Academy rules).

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the Academy open to legal challenge. It is important that authorised staff should have training and sufficient knowledge of electronic devices and data storage.

If inappropriate material is found on the device the Online Safety Incident process, set out in the Trust's e-safety policy, should followed.

Members of staff may require support in judging whether the material is inappropriate or illegal. This will normally be the Principal and DSL. Care should be taken not to delete material that might be required in a potential criminal investigation.

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files if they think there is a good reason to do so (ie the staff member must reasonably suspect that the data or file on the device in question has been, or could be used to cause harm, to disrupt teaching or to break the Academy rules).

If inappropriate material is found on the device, it is up to the Principal to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of Academy discipline) or whether the material is of such seriousness that it requires the involvement of the police.

A record should be kept of the reasons for the deletion of data / files.

Care of Confiscated Devices

Academy staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices (particularly given the possible high value of some of these devices).

Audit / Monitoring / Reporting / Review

The DSL will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files. Appendix 9 provides a template for the recording of the reviewing of internet or electronic devices.

These records will be reviewed by the DSL at regular intervals.

This policy will be reviewed by the Trust in response to changes in guidance and evidence gained from the records.

Appendix 11

GREENWOOD ACADEMIES TRUST

Legislation

Academies should be aware of the legislative framework under which this E-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

General Data Protection Regulation (GDPR) 2018

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept no longer than is necessary
- Processed in a manner that ensures appropriate security

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures. Please read the FOI policies for full information.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The Academy reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice and Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual.

A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against

him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of Trust to engage in sexual activity with any person under 18, with whom they are in a position of Trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of Trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. see template policy in these appendices and for DfE guidance

http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations

Appendix 12

GREENWOOD ACADEMIES TRUST

Filtering Policy

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for e-safety and acceptable use. It is important that the Trust and its academiesl have a filtering policy to manage the associated risks and to provide preventative measures which are relevant and proportionate to the situation in the Trust and its academies.

Many users are not aware that there is some flexibility to filtering services at a local level for academies. Where available, academies can use this flexibility to meet their learning needs and reduce some of the frustrations occasionally felt by users who wish to maximise the use of the new technologies. The Academy Principal (delegated to the E-Safety Officer) or Service Director is responsible for agreeing with Central IT any changes to the standard GAT filtering category list. This should be based on an assessment of any additional risk versus enhancements to the teaching and learning environment.

Responsibilities

The responsibility for the management of the Trust's filtering policy will be held by the IT Director. Central IT will manage all Academy and Central Team filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the Academy filtering service must be agreed by the IT Director upon production of a change request from the Principal, E-Safety Officer or Service Director in the case of the Central Team, which sets out the educational benefits of the change and how the Academy will seek to reduce any risk of any inappropriate exposure to content to pupils and staff. Changes will be logged as a request via the service desk in change control logs specified by the IT Director.

All users have a responsibility to report immediately to the service desk any infringements of the Trust's filtering policy which they become aware of which they believe should have been filtered. The procedure for reporting sites to be blacklisted is outlined in the document 'Internet Filtering Policy and Procedure 23/2/15'. If in any doubt, please report incidents to the service desk immediately by telephone.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. The Trust manages its own filtering service and has provided enhanced / differentiated user-level filtering. This allows different filtering levels for different ages / stages and different groups of users – staff / pupils.

Differentiated internet access is available for staff and customised filtering changes are managed by Central IT. Illegal content is filtered by actively employing the Internet Watch Foundation CAIC category list and other illegal content lists . Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the academy to breaches of the filtering policy, which are then acted upon.

Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with Trust practice.

In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged via the service desk and carried out by a process that is agreed by the Principal or the Service Director in the case of the central team.

Any filtering issues should be reported immediately to the service desk.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through a programme of e-safety education. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Policy
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Digital Citizenship Contract.

Changes to the Filtering System

There is a clear route for reporting and managing changes to the filtering system. Requests from staff for sites to be removed from the filtered list will be considered by E-Safety Officer or Service Director in the case of the central team. If the request is agreed, this action will be recorded and logs of such actions shall be retained by Central IT.

Users with Unfiltered Access

There are a number of staff within the Trust who require unfiltered access to the Internet. These fall into two main groups - E-Safety/DSLs and technical staff. The need can be described as follows:

- To allow E-safety Officers and DSLs to assess content from online services when they need to be able to view a site in its entirety to make a judgment on its suitability
- To allow E-Safety Officers and DSLs to carry out safeguarding duties where access to online services is necessary to gather evidence or assess child protection issues.
- To allow technical staff to assess content from online services when they need to be able to view a site in its entirety to make a judgment on its suitability
- To test technical solutions, diagnose problems and perform security testing, technical staff are required to remove the filtering of sites via the firewall and other filtering systems.

Unfiltered access remains monitored and the access of the individual is traceable. These logs are monitored for misuse.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The Academy will therefore monitor the activities of users on the Academy network and on Academy equipment as indicated in the School E-Safety Policy and the Acceptable Use Policy. Monitoring will take place as follows:

Each month a report of Internet usage by staff that contravenes Trust policy will be sent to the E-Safety Officer at the Academy. The E-Safety Officer will be responsible for discussing transgressions with the user.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to the Chief Executive, Deputy Chief Executive (Safeguarding Lead) and relevant Principal on request.

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision (the evidence might show a large number of requests to remove the filtering from sites – in which case the Trust might question whether its current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring / disciplinary action might be necessary).

Appendix 13

GREENWOOD ACADEMIES TRUST

Links to other organisations or documents

The following links may help those who are developing or reviewing a school e-safety policy.

UK Safer Internet Centre

Safer Internet Centre

South West Grid for Learning

Childnet

Professionals Online Safety Helpline

Internet Watch Foundation

CEOP

http://ceop.police.uk/ ThinkUKnow

Others:

INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm
UK Council for Child Internet Safety (UKCCIS) www.education.gov.uk/ukccis

Netsmartz http://www.netsmartz.org/index.aspx

Support for Schools

Specialist help and support SWGfL BOOST

Cyberbullying

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/

Scottish Government Better relationships, better learning, better behaviour

DFE - Cyber bullying guidance

DfE – Preventing & Tackling Bullying – Advice to school leaders, staff and Governing Bodies

Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm

Cyberbullying.org - http://www.cyberbullying.org/

Social Networking

Digizen – Social Networking

SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people

Connectsafely - Parents Guide to Facebook

Facebook Guide for Educators

Curriculum

SWGfL Digital Literacy & Citizenship curriculum

Glow - http://www.educationscotland.gov.uk/usingglowandict/

Alberta, Canada - digital citizenship policy development guide.pdf

Teach Today – http://www.teachtoday.de/en

Insafe - Education Resources

Somerset - e-Sense materials for schools

Mobile Devices / BYOD

Cloudlearn Report Effective practice for schools moving to end locking and blocking

NEN - Guidance Note - BYOD

Data Protection

Information Commissioners Office:

Your rights to your information – Resources for Schools - ICO

ICO pages for young people

Guide to GDPR - Information Commissioners Office

Guide to the Freedom of Information Act - Information Commissioners Office

ICO guidance on the Freedom of Information Model Publication Scheme

ICO - Guidance we gave to schools - September 2012 (England)

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Hosted Services

Information Commissioners Office good practice note on taking photos in schools

ICO Guidance Data Protection Practical Guide to IT Security

ICO – Think Privacy Toolkit

ICO – Personal Information Online – Code of Practice

ICO – Access Aware Toolkit

ICO Subject Access Code of Practice

ICO – Guidance on Data Security Breach Management

SWGfL - Guidance for Schools on Cloud Hosted Services

LGfL - Data Handling Compliance Check List

NEN - Guidance Note - Protecting School Data

Professional Standards / Staff Training

DfE - Safer Working Practice for Adults who Work with Children and Young People

Kent - Safer Practice with Technology

Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs

Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support

NEN - Guidance Note - esecurity

Working with parents and carers

SWGfL / Common Sense Media Digital Literacy & Citizenship Curriculum

SWGfL BOOST Presentations - parents presentation

Connect Safely - a Parents Guide to Facebook

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

DirectGov - Internet Safety for parents

Get Safe Online - resources for parents

Teach Today - resources for parents workshops / education

The Digital Universe of Your Children - animated videos for parents (Insafe)

Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide

Insafe - A guide for parents - education and the new media

The Cybersmile Foundation (cyber bullying) - advice for parents

Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011

Futurelab - "Digital participation - it's not chalk and talk any more!"

Appendix 14

GREENWOOD ACADEMIES TRUST

Glossary of Terms

AUP	Acceptable Use Policy – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPC	Child Protection Committee

CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
FOSI	Family Online Safety Institute
EA	Education Authority
ES	Education Scotland
HWB	Health and Well-being
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICT Mark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NAACE	National Association of Advisers for Computers in Education
NEN	National Education Network – works with the Regional Broadband Consortia (eg SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational e-safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol