TDAP027E
Acceptable Use of ICT Policy

Requisite: Dorcan Requirement				**Responsible Committee: F&P**	
Vers.	Approval Date	Committee	Head	Chair	Next Review Date
A	01/02/10	*Curriculum*			15/06/11
D	18/06/2018	*Finance and Premises*			01/06/2020
E	26/04/2021	*Finance and Premises*			01/04/2024

Rationale

The Dorcan Academy IT facilities must be used correctly and not misused or abused by users. This includes electronic services such as, but not limited to, email and Internet access. All staff and students should be committed to conforming to good practice in this area. Use of the Academy's IT facilities implies acceptance of the conditions of use. This document sets out current policy and practice; this document is reviewed regularly and can change without notification. Students should also refer to Appendix 3 for specific student requirements.

Purpose

The following regulations apply to users of all IT facilities and learning resources owned, leased or hired by the Academy, all users of such facilities and resources on the Academy's premises and all users of such facilities and resources connected to the Academy's networks. More specific guidance is provided in the Appendices to the policy.

Staff and students should note the consequences of failing to comply with these regulations, particularly that disciplinary action may be taken by the Academy for failure by a user to comply with them and that they may be charged for the Academy's costs arising out of such failure. The Academy is defined as The Dorcan Academy.

Definitions

Portable Computers – Laptops, Netbooks, computers, notebooks and other portable IT devices owned, leased or hired by the Academy.
Desktop Computers – Static Desktop & Workstation computers and IT devices owned, leased or hired by the Academy.
Mobile Technology - owned by staff /students or the Academy.
Users - All staff and students of the Academy and others who have been given permission to use the Academy's IT facilities and learning resources.
Facilities - IT facilities located in the Academy, including networks, servers, desktop computers and portable computers, together with the software and data stored on them. Any IT use carried out on equipment connected to the Academy network, whether or not this involves the use of a Academy-based or Academy-owned device.

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 4)

Learning Resources - All learning resources including (but not exclusively) text, video and audio that is available to the Academy's users.
Designated Authority - The Designated Authority refers to the Academy's Senior Leadership Team (SLT). The Designated Authority may delegate responsibility for particular areas to appropriate Academy staff.

Relevant Legislation

Users must comply with all UK legislation relating to the use of information, computers and networks. Applicable laws include, but are not limited to:

a. **Data Protection Act 1998 and 2018**. This act makes provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.
b**. General Data Protection Regulation (GDPR) 2018** This regulation is largely incorporated into the 2018 DPA and makes further provision for the processing of information relating to individuals.
c. **Copyright, Designs & Patents Act 1988**. Copyright material includes literary works (including computer software), artistic works (including photographs), sound recordings (including music), films (including video) and databases.
d. **Computer Misuse Act 1990**. The act provides safeguards for computer material against unauthorised access or modification.
e. **Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011**. These regulations prohibit the sending of unsolicited marketing emails (or SMS/text messages) to individuals. In addition, the regulations control the use of 'cookies'[1].
f. **Fraud Act 2006**. The Act prohibits 'phishing' whereby official-looking emails guide unsuspecting users to fake websites (e.g. fake bank websites) in order to steal their login or other confidential details. Creating or possessing software to enable this activity is also an offence.

Procedures – sections outlining the procedures and practice in detail including roles and responsibilities

Use of Facilities and Learning Resources:

Personal Use
The Academy's IT facilities are provided for educational, administrative, research and personal development use by staff in the course of their employment and by students in the course of their education. Any other use of the Academy's resources puts an additional demand on those resources, which affects their performance.

Limited personal use of certain facilities is permitted, during personal time. Any such use must neither interfere with the employee's own work or the student's study, nor prevent others from pursuing their legitimate work and use of the Academy's IT facilities. The Academy reserves the right to withdraw this benefit either individually or collectively at any time. In such circumstance the Academy will endeavour to give reasonable notice of its intention to withdraw such benefit.

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 4)

Where the Academy becomes aware of a specific type of personal use which affects the efficient operation of its IT facilities, the Academy will take appropriate steps to withdraw, without notice, access to the relevant facility or resource. Non-exhaustive examples of this include barring access to certain technology or Internet resources such as web sites, news groups or other Internet resources. Users who have a legitimate requirement to access such withdrawn resources should discuss the matter with the Designated Authority. The fact that a user is able to access a particular technology or resource does not necessarily imply that the technology or resource may be accessed in accordance with these Regulations.

Commercial Use
Use of any of the Academy's IT facilities for commercial gain (including advertising) or for work on behalf of others (unconnected with a student's course of study at the Academy or a member of staff's legitimate activities) is prohibited, unless the User has explicit prior written permission of the Designated Authority and an appropriate charge for such use has been contractually agreed between the other party and the Academy.

Movement
Academy IT facilities, with the authorised exception of portable devices should not be moved or disconnected without the prior agreement of the Designated Authority.

Connection - Network Access

Users must not connect any personal device into the Academy's network or other IT facility without prior agreement from the Designated Authority.

Damage
Users must not cause any form of damage to the Academy's IT facilities, software, or to any of the rooms and their facilities and services which contain that equipment or software. The term 'damage' includes any unauthorised installation of hardware or software, which incurs time and/or cost in restoring the facilities to their original state.

Security
Users must not deliberately introduce any virus, worm, Trojan horse or other harmful or nuisance program or file into any IT facility, nor take deliberate action to circumvent any precautions taken or prescribed by the Academy to prevent this. Users must also take adequate precautions (due diligence) to avoid accidental introduction of harmful software such those previously mentioned. Users must not attempt to penetrate the security and/or privacy of other users' files. All of the Academy's IT facilities have anti-virus and anti-spyware protection installed.

Spam and Mass-circulation
Spam is usually defined as unsolicited electronic messages (using email, SMS, Instant Messaging or other means) sent in bulk. Users may not use Academy IT facilities to send Spam.

Sending unsolicited electronic messages for the purposes of marketing is prohibited under the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011.

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 4)

Illegal and/or Offensive Material

Users must not use Academy IT facilities to access, produce, obtain, download, store, view, share, or distribute material (including images, video, text or sound files) which is either illegal under UK law (e.g. in breach of copyright law) and/ or can reasonably be judged to be offensive, likely to incite racial hatred, obscene, indecent, or abusive. The only exceptions would be where such material, which may be judged offensive, is essential for research or teaching, is permitted by law, and prior permission has been granted by the Designated Authority. If illegal or offensive material is received, the designated authority should be notified, and the material deleted immediately and not forwarded.

Discrimination

Users must not use the Academy's IT facilities to place, disseminate or receive materials which discriminate or encourage discrimination on, for example, the grounds of gender, sexual orientation, disability, age, religious belief, race or ethnic origin.

Defamation

Users must not use the Academy's IT facilities to publish any information they know or believe to be untrue, is defamatory and could not be defended on the grounds that it is true/factual or that it is fair comment on a matter of public interest (e.g. works of literature, art, music, television and radio or the activities of public figures).

Monitoring of IT Facilities

In order to protect the security and working of the Academy's IT facilities & users, it may be necessary to monitor collective or individual usage of its IT facilities. This is particularly likely where there are indications of abuse of systems, or that individuals may be using systems in excess of their authority. Files, messages, emails and user account information may be intercepted, monitored, recorded, copied, audited, and inspected.

Confidentiality

Absolute confidentiality cannot be guaranteed. Any emails or files, stored and/or sent or received may be accessed by colleagues other than the individual to whom it was intended for, whether by accident (e.g. a computer left logged on) or design (e.g. an email may need to be opened to diagnose connectivity problems which have been brought to the attention of the IT Support department.). Emails and files cannot therefore be regarded as totally private or confidential. Personal email messages and files should be written remembering this possibility for third parties to review the content. In the case of external (Internet) Email, there cannot be an absolute guarantee of security. Such emails can potentially be intercepted and read by third parties without our knowledge. Messages of particular confidentiality or sensitivity should be sent by an alternative medium. Data Protection and GDPR Regulations must be observed.

The IT Support department have total administrative access to all of the Academy's IT facilities. The IT Support department have the right to monitor and access all IT resources, this includes any saved files. Any misuse of IT facilities found by the IT Support department will be reported to the Designated Authority.

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 4)

Internet Access

Internet access is provided for educational, administrative, research and personal development use. It should be noted that users of the Internet do not have a right to confidentiality or privacy when using or accessing the Academy's IT facilities. The Designated Authority monitors and reviews network logs maintained in order to ensure compliance with Academy policies and UK law. The Academy uses monitoring software to track usage. This software records details of every web site visited, along with the relevant user name and date/time, and produces regular reports for monitoring purposes. Misuse, or visits to sites of an improper nature, will automatically be reported to the Designated Authority. Use of the Academy Wi-Fi is for authorised persons only.

Social Media

The Academy must not be exposed to legal and governance risks that may adversely affect the Academy's reputation. Users should be able to see that only legitimate representations are being made via social media and the correct protocols must be applied where employees are authorised to contribute to any social networking application.
The Designated Authority will determine the level of access allowed at the Academy, however, individuals may choose to use social media in their personal time. All employees must understand however, that they hold a position of responsibility in the public domain therefore the implications of inappropriate use that may result in disciplinary action if the use is detrimental to the reputation of the Academy or causes damage to the Academy, any of its employees or a third party's reputation may amount to misconduct or gross misconduct and could lead to dismissal. Employees must also understand that information shared through social media is subject to copyright, Data Protection and Freedom of Information legislation and the Safeguarding Vulnerable Groups Act 2006. Employees must also operate in line with Academy Policy.
Anyone who becomes aware of inappropriate postings on social networking sites, must report it to their line manager as soon as possible. The line manager will then follow the disciplinary procedure. If an employee fails to disclose an incident or type of conduct relating to social networking sites, knowing that it is inappropriate, may be subject to the disciplinary procedure.
It is unacceptable for any employee to discuss pupils, parents, work colleagues or any other member of the Academy community on any type of social networking site. Reports about oneself may also impact on the employment relationship - for example if an employee is off sick, but makes comments on a site suggesting the contrary.
Please refer to Appendix 1 for further guidance on the use of Facebook and Social Media.

Email

The Academy reserves the right to retrieve the contents of messages for the following purposes:

- to monitor whether the use of the e-mail system is legitimate and in accordance with this policy;
- to find lost messages or to retrieve messages lost due to computer failure;
- to assist in the investigation of wrongful acts;
- to comply with any legal obligation.

Monitoring will only be carried out to the extent permitted or required by law. The Academy will

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 4)

not routinely monitor e-mail messages. Spot checks or tailored searches may be undertaken in the context of disciplinary proceedings (whether actual or contemplated) or where the Academy has reason to believe that the systems may be being used in breach of this policy.

The Academy's policy towards spam is that it should be filtered upon receipt and quarantined. All effort is made to filter out spam before reaching users' inboxes, however it should be kept in mind that spam filtering is an ongoing endeavour and therefore not fool-proof. The occasional message may reach a user and should be deleted in the normal way. Measures are taken to ensure that no false-positives (legitimate messages treated as spam) are filtered; however it is possible that the occasional message is falsely identified as spam. In such cases the quarantine email can be released by the IT Support department.

Please also refer to Appendix 2 for email usage advice

Files

The Academy reserves the right to retrieve the contents of files for the following purposes:

- to monitor whether the use of the storage medium is legitimate and in accordance with this policy;
- to find deleted files or to retrieve files lost due to IT facility failure;
- to assist in the investigation of wrongful acts;
- to comply with any legal obligation.

Monitoring will only be carried out to the extent permitted or required by law. The Academy will not routinely monitor files. Spot checks or tailored searches may be undertaken in the context of disciplinary proceedings (whether actual or contemplated) or where the Academy has reason to believe that the systems may be being used in breach of this policy.
Please note that the IT Support department have administrative privileges and access to your personal folder and all files stored on the Academy's IT facilities. Please do not store personal photos, music or documents in personal folders; it is designed for storing work documents only.

Software

Users of the Academy's network are not authorised to and are unable to load any software onto the IT facilities. Only software licensed to the Academy may be installed on the Academy's IT facilities. It is forbidden, under any circumstances, to load any software onto any device or network owned or hired by the Academy without prior consent from the Designated Authority. It is also forbidden to run peer to peer (P2P) software on any of the Academy's IT facilities. It is also prohibited to run anonymising or non-Academy VPN software.
Software downloaded from the Internet and/or software obtained illegally must not be loaded onto the Academy's IT facilities. Any software obtained and/or installed illegally will be reported to the Designated Authority.

Maintenance & Repairs

Maintenance is to be controlled by the IT Support Department in conjunction with external suppliers. From time to time IT facilities - especially portable devices - will be recalled by IT Support for maintenance purposes. It will not be possible to properly support the Academy's IT

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 4)

Facilities if equipment is not correctly maintained. Any faulty/out of order IT facility should be reported to the IT Support department as soon as the problem is found. Any data stored on faulty IT facilities will be recovered using a "best effort" approach by the IT Support department. Any cost incurred by the IT Support department in recovering data may be charged back to the user or department involved.

If any IT facilities require external repair, The IT Support department will take a "best effort" approach to remove all data ahead of repair.

Copyright and Licence Agreements

Users must adhere to the terms and conditions of all licence agreements relating to IT facilities and learning resources, which they use including software, services documentation and other goods.
Users must not copy or modify any copyright material (3rd party material) nor incorporate any part of the 3rd party material into their own work unless such acts are either permitted under the CDP Act 1988, by a Licence Agreement, or with the permission of the copyright holder.
Users must not install, make, store, or transfer unlicensed copies of any copyright or trademark work including software, videos or music, unless permitted under legislation or with the permission of the copyright holder.

Behaviour

Users must respect the rights of others and should conduct themselves accordingly when using IT facilities to create a beneficial environment for all.
Users must not interfere with or disrupt the availability and use of the IT facilities by others.
Users must take every precaution to avoid damage to equipment and learning resources caused by the presence of food and drink in its vicinity. Under no circumstances must food or drink be consumed near any IT facilities.

Infringement

Withdrawal of facilities - If a User is in breach of any of these regulations, the Designated Authority may withdraw or restrict the User's use of IT facilities and learning resources, following consultation with the User's head of department or in relation to students, their form tutor, head of year/house and/or parents.

Removal of Material - The Academy reserves the right to remove material from its IT facilities without notice where such material is in breach of these regulations.

Disciplinary action - Any breach of the regulations may be dealt with by the Designated Authority under the Academy's formal disciplinary procedure for both students and staff and in some cases may result in suspension, expulsion or dismissal. The User may be charged for any costs that have arisen as the result of misuse or abuse of facilities and/or resources.

Breaches of the law - Where appropriate, suspected breaches of the law may be reported to the police. Where the breach has occurred in a jurisdiction outside the UK, the breach may be reported to the relevant authorities within that jurisdiction.

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 4)

Disclaimer

The Academy accepts no responsibility and expressly excludes liability to the fullest extent permissible by law, for:

- The malfunctioning of any IT facility or part thereof, whether hardware, software or other.
- The loss of any data or software or the failure of any security or privacy mechanism.

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 4)

Appendix 1

Staff Guidelines for the use of Facebook.com and other social media platforms
General Practice and Advice

- Members of staff should not be in contact with current students via social networking sites such as Facebook.com, in accordance with the Academy's Safeguarding and Welfare policy.
- Members of staff with Facebook profiles should set the privacy levels on their accounts to maximum i.e. only people on their friend's list should be able to view their pictures/private information etc. This can be done by going to **Setting** > **Profile** and adjusting the parameters accordingly.
- Members of staff with distinctive surnames should be aware that it will be relatively easy for students to find them on Facebook i.e. due to the large number of people named John Smith it is difficult to trace a specific individual.
- Members of staff should note that although these measures will make it harder for students to find them on Facebook a determined individual with knowledge of how the website works will eventually be able to trace a person (given enough time).

Action to be taken if a member of staff is contacted by a student.

There are two types of contact through Facebook:

- A message
- An invitation to be added to a person's "Friends list"

If a message from a student is received the following action should be taken:

- **Do not reply to the message.** Replying to a message allows the recipient to view your profile in its entirety. This also circumvents the privacy settings on account.
- A senior member of staff should be contacted at the earliest opportunity and informed of the incident.
- Pastoral staff should then be asked to speak to the student on behalf of the member of staff who was contacted. The relevant Facebook correspondence should be made available to the pastoral staff dealing with the situation to aid in any investigation.
- The student should be reminded of the Academy's ICT Acceptable Use policy and that contacting staff in this manner is inappropriate. A note for file and notification to parents should also be made.

If invited to a student's friends list the following action should be taken:
Immediately reject the invitation.

- A senior member of staff should be contacted at the earliest opportunity and informed of the incident.
- Pastoral staff should then be asked to speak to the student on behalf of the member of staff who was contacted. The relevant Facebook correspondence should be made available to the pastoral staff dealing with the situation to aid in any investigation.
- Note that rejection of a "friend request" allows the sender to repeat the action; if this occurs the relevant members of pastoral staff should be made aware of this.
- The student should be reminded of the Academy's ICT Acceptable Use policy and that contacting staff in this manner is inappropriate. A note for file and notification to parents should also be made.

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 4)

Appendix 2

Email – Good Practice

The nature of the Dorcan Academy site and the busy schedules led by all who work here mean that email can be a vital tool of communication. However, it is not for fostering positive face to face relationships with colleagues. Email should not be regarded as a replacement for formal meetings or more informal conversations on the telephone or at staff briefings, break or lunch. The aim of this brief guide is to provide some suggestions on the way that email can be used most effectively and to improve the experiences of all those who interact electronically.

Is it necessary?

People are busy. Your message may be one of tens or hundreds for a recipient to deal with depending on how busy they are, how many lessons they have taught that day, how many extra-curricular activities they have been organising. If they are receiving so many messages, what are the chances that they will read your message with great care, particularly if they perceive it to be only tangentially relevant to them? For many people, email is fast becoming a chore not a vital tool of communication. Do not accelerate this process by contributing messages / information that could be broadcast or communicated in another, often more efficient, way.

Beware of Forwarding

Consider carefully the necessity of forwarding a message and to whom. Consider and adhere to the data sharing regulations under GDPR. Take great care with any attachments, even from senders well known to you. Encrypt sensitive attachments with separately shared passwords. When forwarding, include a summary of what you are sending – tell the recipients what it is in a sentence or two. If it is worthwhile to forward, it's worth an extra moment of your time to summarise your reason for forwarding.

Copying in/Blind copying

Be aware that sometimes it might be inappropriate to copy others into an email. Colleagues may not want personal email addresses shared. Don't share personal addresses in global emails unless specifically given permission to do so. Bcc can be used if necessary.

Dealing with Emotions

One of the attractions of email communication is that it can be quick and simple. However, this can also be a weakness. When you are writing letters, the very nature of the activity forces you to think about your choice of language. You may even go through a draft or two
– considering carefully the impact of your words on the reader. Emails are often drafted all too rapidly and immediately sent off. Emotions or nuances you may feel were obvious could be missed by the recipient or perhaps they may read into your message and pick up attitudes or meaning that you had no intention of conveying. Humour is notoriously tricky to convey appropriately via Email, even to people that you know well. Therefore, the following suggestions can be useful:

Don't Criticise

Never chastise or criticise someone via an electronic communication. Even well-meaning and

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 4)

constructive criticism can hit home much harder on screen when you are not there to moderate the blow with body language, vocal tone and flexible response to the observed reaction. Even if you do not feel that you are criticising – perception of a message must always be carefully considered.

Cool Off

If you have something to get off your chest, write the email message then save it for a few hours / a day then re-read it. In the meantime, circumstances may change or you may have an opportunity to talk to the person causing your anxiety. Even if little has changed, it is highly likely that you will edit or re-write your original Email and it will be a more effective message for the greater sense of detachment and objectivity the extra reflection time has provided. Get out of the habit of a quick send then lengthy regret.

Take Care

Before responding to any email message, re-read it to ensure that you fully understand it. Many messages are sent / forwarded without the reader really grasping the point and responding appropriately. Try to get into the habit of proof-reading your own messages. This will ensure that your meaning and your requirements are clear and should help to minimise the chance of misunderstanding or frustratingly irrelevant replies.

Writing the Email

Clear entries in the subject guides to assist the reader in prioritising their inbox and sharp, concise email messages all play their part in making the process efficient and painless. Avoid putting too much information into one message – your key points may become buried. Email is, by its very nature, designed for short, digestible snippets of information. Readers do not expect tomes and they do not expect additional information beyond the subject guide. If you have lots to say then it may be lost in a long message – consider breaking it down into several messages or communicating your concerns in a different fashion.

Urgency and Reliability

Email feels immediate. It is not. It is subject to both technical system and reader variables. All staff should try to check their Email twice a day but, as we all know, sometimes this is not possible. Even when it does happen it is most likely to occur at 8a.m., lunchtime or after 4p.m. bear this in mind when you send a message in the hope of a speedy reply by return. Try the phone. If it is urgent, check staff timetables and seek people out.

Email Conversations

If your email exchange on one topic results in two or more "cycles" then it is probably best to stop and talk to each other. Email will simply take too long and the subject is obviously knotty / complex enough to need a proper form of exchange with much more interactive feedback.

Email communication to parents

These should always be discussed with Heads of House in advance of any reply and a record of the exchange placed on the student's file. If in doubt about any other external contact – speak to a member of SLT.

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 4)

Appendix 3

Policy Overview for Students

- With the exception of portable computers, IT equipment should not be moved, relocated or adjusted without the permission of a member of staff.
- Smartboards and Projectors should not be touched without a member of staff present in the classroom in order to supervise.
- No software should be installed onto any computer at the Academy.
- If you accidentally damage or find damaged IT equipment, please report it to the IT Support department or a member of staff immediately.
- Internet access is provided for educational, research and personal development use. If students abuse this by seeking out sites that do not meet these objectives, they may be subject to appropriate disciplinary sanctions. Use of the Academy network is carefully monitored and recorded.
- Students should not make contact with members of staff on Facebook or any other social media other than through authorised channels set up by the Designated body.
- Every student has an area to store private files and folders. If your work is important, please save additional copies elsewhere as the Academy cannot guarantee against possible hardware failure. In order to maintain the efficiency of the system network administrators can, if necessary, gain access to your Home Space. Therefore, do not store any personal photos, music or documents as your Folders are designated for Academy work only.
- Any deliberate attempt to damage or 'hack' into the Academy's IT infrastructure will result in serious disciplinary action that may include temporary or permanent exclusion from Academy.
- The use of mobile phones, IPhones and any music device is at the discretion of teachers in support of quality teaching & Learning.
- The Dorcan Academy uses web filtering software to secure, monitor and limit certain websites for your security. However, if you feel that we have blocked a legitimate website then please let the IT Support department or your teacher know.

Cyber-bullying

The Academy regards cyber-bullying, through the inappropriate use of electronic communication such as text messages, email or postings on social networking websites like Facebook, as an unacceptable form of bullying. This includes the use of technology outside of normal Academy hours if it interferes with the safety and wellbeing of any member of the Academy community. Such incidents will be treated seriously, investigated thoroughly and appropriate disciplinary measures taken if necessary.

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 4)

Appendix 4

The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies

- Complaints
- Safeguarding Children and Young people
- Behaviour
- Anti-Bullying
- Lettings and Use of Premises
- Special Educational Needs
- Academy trips
- Curriculum
- Children in Care
- Health and Safety
- Sex and Relationships Education
- Security
- E-safety
- Equality Diversity and Community Cohesion
- Students with Medical Needs
- Internet Access and Use
- Acceptable Use of ICT
- Cloud based
- Data Protection
- Password
- Digital Images
- Anti-Fraud & Corruption
- Young Carers
- Privacy, Confidentiality, Information Sharing and Data
- Whistle blowing

The above list is not exhaustive but when undertaking development or planning of any kind the Academy will to consider safeguarding matters.

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 4)

- **Revision Notes**

Rev A	original
Rev B	Amendments made in line with Academy procedures. Approved by the Curriculum Committee on 1/05/2013 and ratified by the Full Governing Body on 22/05/2013
Rev C	update to general wording and legal references. Agreed and approved by the Finance and Premises Committee 19 June 2017
Rev D	To incorporate GDPR changes. Agreed and approved by the Finance and Premises Committee 18 June 2018
Rev E	Reviewed policy in line with policy schedule. Agreed and approved by the Finance and Premises Committee 26/04/2021

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 4)